KIESEL BOUCHER LARSON LLP
Paul R. Kiesel (SBN 119854)
kiesel@kbla.com
8648 Wilshire Boulevard
Beverly Hills, CA 90211-2910
Telephone: (310) 854-4444
Facsimile: (310) 854-0812
Interim Liaison Counsel

BARTIMUS, FRICKLETON, ROBERTSON & GORNY, P.C.
Edward D. Robertson, Jr.
Stephen M. Gorny
James P. Frickleton
Mary D. Winter
Edward D. Robertson III
11150 Overbrook Road, Suite 200
Leawood, KS 66211
chiprob@earthlink.net
Telephone: (913) 266-2300
Facsimile: (913) 266-2366
Interim Co-Lead Counsel

STEWARTS LAW US LLP
David A. Straite. (admitted *pro hac vice*)
Ralph N. Sianni
Michele S. Carino
Lydia E. York
1201 North Orange Street, Suite 740
Wilmington, DE 19801
dstraite@stewartslaw.com
Telephone: (302) 298-1200
Facsimile: (302) 298-1222
Interim Co-Lead Counsel

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

FIRST AMENDED CONSOLIDATED CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

NATURE OF THE ACTION

1. This class action lawsuit, seeking in excess of $15 billion in damages and injunctive relief brought by, and on behalf of, similarly situated individuals domiciled in the United States who had active Facebook, Inc. ("Facebook" or the "Defendant") accounts from May 27, 2010 through September 26, 2011 (the "Class Period"), arises from Facebook's knowing interception of users' internet communications and activity after logging out of their Facebook accounts in violation of state and federal laws.

JURISDICTION AND VENUE

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

3. This Court has subject matter jurisdiction over this action and Defendant Facebook pursuant to 28 U.S.C. § 1331 because this action arises in part under federal statutes, namely the Federal Wiretap Act, 18 U.S.C. § 2511 (the "Wiretap Act"), the Stored Communications Act, 18 U.S.C. § 2701 ("SCA") and the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (the "CFAA") and pursuant to 28 U.S.C. § 1332(d) because the amount in controversy exceeds $5,000,000.

4. 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 governs the relationship between Facebook and its users, provides for exclusive venue in state or federal courts located in Santa Clara County, California.

THE PARTIES

5. Plaintiff Mrs. Perrin Davis ("Davis") is an adult domiciled in Illinois. Davis had an active Facebook account during the entire Class Period, which Facebook utilized to track and intercept her specific electronic activity and communications.

6. Plaintiff Prof. Cynthia Quinn ("Quinn") is an adult domiciled in Hawaii. Quinn had an active Facebook account during the entire Class Period, which Facebook utilized to track and intercept her specific electronic activity and communications.

7. Plaintiff Dr. Brian Lentz ("Lentz") is an adult domiciled in Virginia. Lentz had an active Facebook account during the entire Class Period, which Facebook utilized to track and

intercept his specific electronic activity and communications.

8. Plaintiff Mr. Matthew Vickery ("Vickery") is an adult domiciled in Washington State. Vickery had an active Facebook account during the entire Class Period, which Facebook utilized to track and intercept his specific electronic activity and communications.

9. Defendant Facebook is a Delaware corporation which maintains its headquarters at 156 University Avenue, Palo Alto, California 94301. 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.

FACTUAL ALLEGATIONS

I. FACTUAL BACKGROUND

> ***Zuckerberg****: Yeah so if you ever need info about anyone at Harvard*
>
> ***Zuckerberg****: Just ask.*
>
> ***Zuckerberg****: I have over 4,000 emails, pictures, addresses, SNS*
>
> ***[Redacted Friend's Name]****: What? How'd you manage that one?*
>
> ***Zuckerberg****: People just submitted it.*
>
> ***Zuckerberg****: I don't know why.*
>
> ***Zuckerberg****: They "trust me"*
>
> ***Zuckerberg****: Dumb fucks.*
>
> \- Facebook Founder Mark Zuckerberg's Instant Messages,
> circa 2004, as made public by New York Magazine
> on September 20, 2010

10. 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.

/ / /

11. Facebook has become the largest social networking site in the world with over 800 million users world-wide and over 150 million users in the United States.

12. Facebook's enormous financial success is the result of connecting advertisers with its huge repository of personal data provided by users. As Facebook explained in its recent Registration Statement, "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.

13. Indeed, in the past three years, over 90% of Facebook's revenue was attributable to third party advertising (see Registration Statement at 13), and Facebook is 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).

14. Although Facebook does not require its members to pay a monetary subscription fee, membership is not free. Instead, Facebook conditions its membership upon users providing sensitive and valuable personal information to Facebook upon registration, including name, birth date, gender and email address. More importantly, Facebook conditions membership upon the user accepting numerous Facebook small text files, called cookies, on the user's computer, which allows Facebook to intercept its users' electronic communications and track browsing history.

15. According to a recent report by Rainey Reitman at the Electronic Frontier Foundation ("EFF"), titled "Facebook's Hotel California" (Oct. 10, 2011), Facebook installs two types of cookies on members' computers:

> ***Session cookies*** *are set when you log into Facebook and they include data like your unique Facebook user ID. They are directly associated with your Facebook account. When you log out of Facebook, the session cookies are supposed to be deleted.*
>
> ***Tracking cookies*** *- also known as persistent cookies - don't expire when you leave your Facebook account. Facebook sets one tracking cookie known as 'datr' when you visit Facebook.com, regardless of whether or not you actually have an account. This cookie sends data back to Facebook every time you make a request of*

> *Facebook.com, such as when you load a page with an embedded Facebook 'like' button. This tracking takes place regardless of whether you ever interact with a Facebook 'like' button. In effect, Facebook is getting details of where you go on the Internet.*
>
> *When you leave Facebook* without *logging out and then browse the web, you have both tracking cookies and session cookies. Under those circumstances, Facebook knows whenever you load a page with embedded content from Facebook (like a Facebook 'like' button) and also can easily connect that data back to your individual Facebook profile.*

As the EFF noted, Facebook promised to delete session cookies upon logout. This is not just vague industry expectation: ***it is the limit of the user's consent under the governing contracts, and therefore under federal law***.

16. Use of Facebook is governed by the Statement of Rights and Responsibilities and several other documents and policies, including a Data Use Policy and a Privacy Policy (hereafter referred to collectively as "governing documents"). Although the governing documents reflect that users consent to Facebook installing cookies on each user's computer, and although users consent to these cookies tracking and transmitting data to Facebook regarding each user's web browsing, such consent was limited to internet usage while users are logged on to Facebook. Users do not consent to Facebook tracking their web browsing activity after logging out of Facebook. In fact, Facebook represented it would delete the session cookies at the time of logout. On Facebook's online help center, Facebook clearly and unambiguously emphasized, "When you log out of Facebook, we remove the cookies that identify your particular account."

17. Even though Facebook assures its users that it does not track their internet browsing post log out, Facebook has been doing exactly that.

18. On September 25, 2011, Australian blogger Nik Cubrilovic reported that: "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."

19. In response, on September 26, 2011, Facebook engineer Gregg Stefancik thanked Cubrilovic "for raising these important issues" and acknowledged that a particular cookie, the a_user cookie, was not cleared on logout, advising that "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."

20. While its response was seemingly forthcoming, Facebook failed to tell users that it had known for nearly a year that its systems were surreptitiously capturing users' internet browsing habits after logout – and moreover, it had been developing better post-logout tracking devices that were designed exactly for that purpose.

21. In fact, Cubrilovic first discovered that Facebook cookies were tracking user's internet usage even after logging out of Facebook without the knowledge or consent of the user in 2010. 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. In short, Cubrilovic established that Facebook was in fact secretly tracking its users' web browsing without their knowledge or consent even after logout.

22. Cubrilovic repeatedly contacted Facebook to report his findings and ask them to fix the problem. For example, Cubrilovic emailed Facebook on November 14, 2010, and then again on January 12, 2011. Facebook refused to respond.

23. Following the findings of Nik Cubrilovic, Facebook admitted that it has been tracking, collecting, storing and using its users' wire and/or electronic communications while users have been logged-out of Facebook.

24. On September 28, 2011, U.S. Representative Edward Markey and U.S. Representative Joe Barton, Co-Chairmen of the Congressional Bi-Partisan Privacy Caucus, submitted a joint letter to the Chairman of the Federal Trade Commission stating, "[I]n this instance, Facebook has admitted to collecting information about its users even after its users had logged out of Facebook."

25. Neither Facebook users nor the third-party websites have given consent or otherwise authorized Facebook to intercept, acquire, store and track users' electronic communications while not logged-in to Facebook.

/ / /

/ / /

26. Facebook has made inconsistent public statements regarding the reason for its post log-out tracking, despite its admission that such tracking occurred. For instance:

1. Facebook first claimed that the post log out tracking of its users' personally identifiable information was "inadvertent" and was a "bug." On October 4, 2011 Facebook Spokesperson Greg Stefancik commented on an online post stating, "as we discussed last week, we are examining our cookie setting behavior to make sure we do not inadvertently receive data that could be associated with a specific person not logged into Facebook." Further, in response to Nik Cubrilovic's blog post, Facebook responded by saying, "What you see in your browser is largely typical, except a_user which is less common and should be cleared upon logout (it is set on some photo upload pages). There is a bug where a_user was not cleared on log out. We will be fixing that today."

2. Facebook then publicly stated that it uses post log-out tracking of specific personally identifiable information for safety purposes only. In a USA Today article, Facebook engineering director Arturo Bejar claimed that Facebook uses such data only to boost security and improve how 'Like' buttons and similar Facebook plug-ins perform.[1]

27. The German Hamburg Commissioner for Data Protection and Freedom of Information conducted a full investigation into Facebook's tracking of users post log-out. Facebook told the Hamburg Commissioner that it "needs" users to be identifiable after log-out for security purposes, but the Hamburg Commissioner was unconvinced. The Hamburg Commissioner issued a press release regarding their investigation, which stated:

> Facebook's argument that all users need to be identifiable even once they have logged out of Facebook in order to guarantee the security of the service is untenable within this context. The fact that the installation of cookies in reality only permits the collection of the user's personal data required to use the service seems extremely questionable. The results of the investigation raised the suspicion that Facebook is creating user tracking profiles.

28. Additionally, a patent application assigned to Facebook, which the U.S. Patent & Trademark Office recently published, indicates that Facebook is not only aware that its cookies persist after logout, but that it deliberately designed them to function in that manner.

[1] *See* Byron Acohido, "How Facebook tracks you across the Web," USA Today, November 16, 2011.

29. Specifically, on February 8, 2011, three individuals, Kent Matthew Schoen, Gregory Luc Dingle and Timothy Kendall, filed a patent application entitled, "Communicating Information in a Social Network System about Activities from Another Domain."2 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.

30. 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 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 website 140, 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

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

> 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 website140.

Patent Application at 5.

31. Further, in certain circumstances, Facebook has to actively bypass 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 to third parties, namely advertisers. This is all done whether the Facebook user is logged onto the social networking site or logged off.

32. 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.

33. 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, one of the three individual applicants, Timothy Kendall, is not an inventor or a computer scientist at all. Rather, Mr. Kendall is the Director of Monetization at Facebook. According to his LinkedIn profile, Mr. Kendall's job at Facebook is "Product Strategy & Development for Facebook's revenue generating products." Essentially, he figures out new and better ways to sell user information to advertisers.

34. In a November 10, 2011 letter, U.S. Representatives Markey and Barton stated, "This patent application raises a number of questions about whether Facebook tracks its subscribers on websites other than Facebook, regardless of login status, or has plans to do so…Experts who have reviewed Publication #20110231240 agree that the patent contemplates tracking users on other websites. The patent also includes sending targeted advertisements to users based on information gleaned from such tracking."

35. On December 21, 2011, Facebook responded to U.S. Representatives Markey and Barton's letter with their own 6-page letter. This letter talked extensively about how their current business operation did not track users while the user was logged-off, but did not discuss their previous tracking systems.

36. In a press release by U.S. Representative Markey's office dated January 9, 2012, the Congressman stated, "Lawmakers are unsatisfied with responses of social networking site to queries about recent patent application that suggests tracking of users on other websites, using information to target advertisements…the main questions of whether Facebook has considered using third-party tracking data to build user profiles or employs user-provided data to target advertising remain unanswered from the company's response to our letter."

37. The press release also states, “Additionally in its response to us, Facebook states that it uses consumer-provided data for ‘internal operations, including data analysis, research, development, and service improvement’ yet provides no description of what these activities entail or how they affect consumer privacy… Facebook seems to be saying one thing and doing another…In the company’s response, it talks a lot about how they don’t currently ‘track’ users online, but they just asked for a patent that would allow them to do just that. Why ask for something you don’t ever plan on using?”

II. HOW FACEBOOK TRACKS ITS MEMBERS’ INTERNET USE

A. How Cookies Are Installed On Users’ Computers

38. On the Web, servers store information on users’ computers via cookies. A cookie is a small text file that the server creates and sends to the browser, which stores it in a particular directory on the user’s computer. Some cookies relate to the browser and others relate to specific users.

39. When a user contacts a web server, such as Facebook, the browser software checks to see if that server has set any cookies on that client machine. If there are valid (unexpired) cookies that were set by that server, then the client sends the cookies to the server. Thus, cookies allow servers to store information on a browser.

40. Because cookies are small text files, there is a limited amount of information that can be stored in them. Typically, servers create database records on the server that correspond to users, sessions, and browsers. These records are indexed by numbers, typically random, and the numbers are the actual values stored in the cookies.

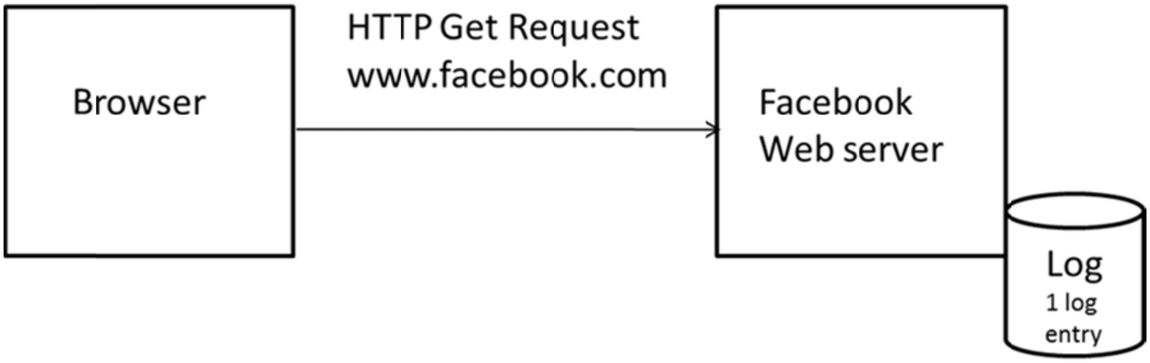
41. Every time that a server, such as Facebook, receives a cookie, the server knows that it is interacting with a client with whom it has interacted before. The server examines the cookie to identify the value of a database index and uses the index value from the cookie to locate the database record that corresponds to that user, session or browser, depending on the type of cookie that is received. For example, a c_user cookie contains an index into a database of information about a particular user who is logged into Facebook.

/ / /

42. When an internet user signs up for Facebook at Facebook.com, the Facebook.com web server implants a number of cookies onto the internet user's computer. The process by which that occurs is as follows:

43. The user types the URL facebook.com in the address bar of his browser.

44. The browser initiates a GET request to the Facebook server to display the webpage. Facebook creates a log file of the request, which is indexed by a number, e.g. 12345:



45. Facebook responds by sending the content of the webpage (an HTTP response containing an HTML page), which is then displayed on the user's browser screen.

46. Facebook's response includes a "Set-cookie" header that causes the browser to store a datr cookie on the user's machine with the value 12345.

47. The Facebook.com homepage is displayed with the possibility to log on or to create an account.

48. Thus, at the end of the response from Facebook, the browser has a datr cookie file, and the Facebook database has an entry that corresponds to that cookie.

/ / /

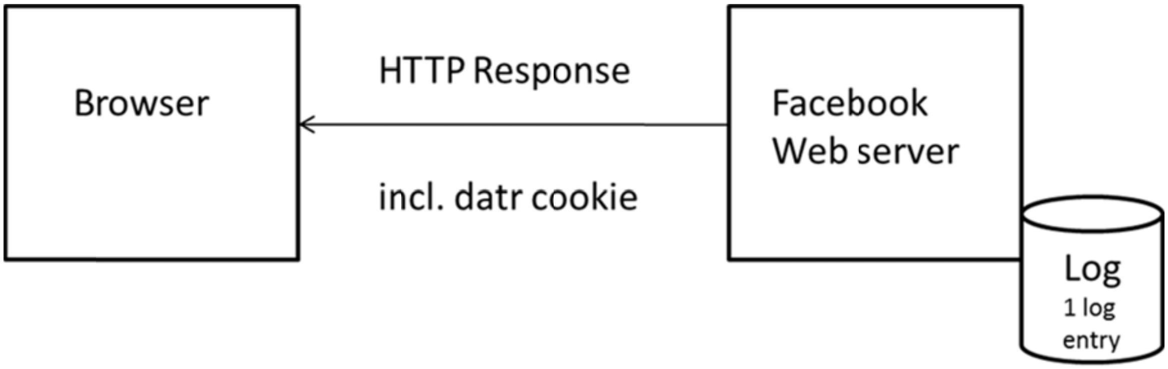
/ / /

/ / /

/ / /

/ / /

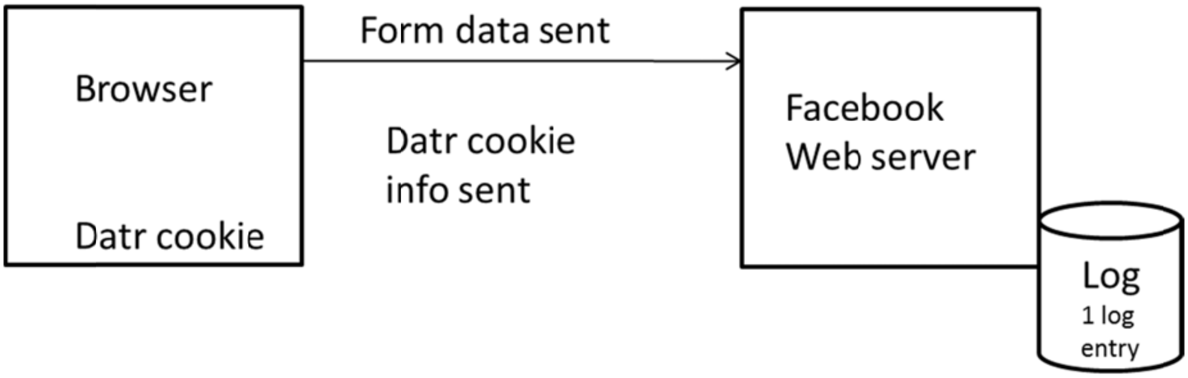
/ / /



49. The user creates an account by entering some private information and clicking the ‘Signup’ button.

50. Clicking this button implies that the user agrees to the Terms of Service of Facebook.

51. The click initiates an HTTP request from the user’s browser to the Facebook server. The browser checks the cookie directory on the client machine to see if there are any cookies for the Facebook.com domain and finds the datr cookie that was recently set there. The cookie with value 12345 is sent to Facebook, along with the GET request, to store the data in a log file and show the next page.



52. When Facebook receives this request, it uses the index 12345 to link the request to the previous request sent by the browser, and in this manner, Facebook can track all subsequent requests from the browser whenever it receives the *datr* cookie with value 12345. If a different browser on a different machine used by a different user interacts with Facebook, the *datr* cookie value sent will be different. As more people connect to Facebook, the size of the database grows,

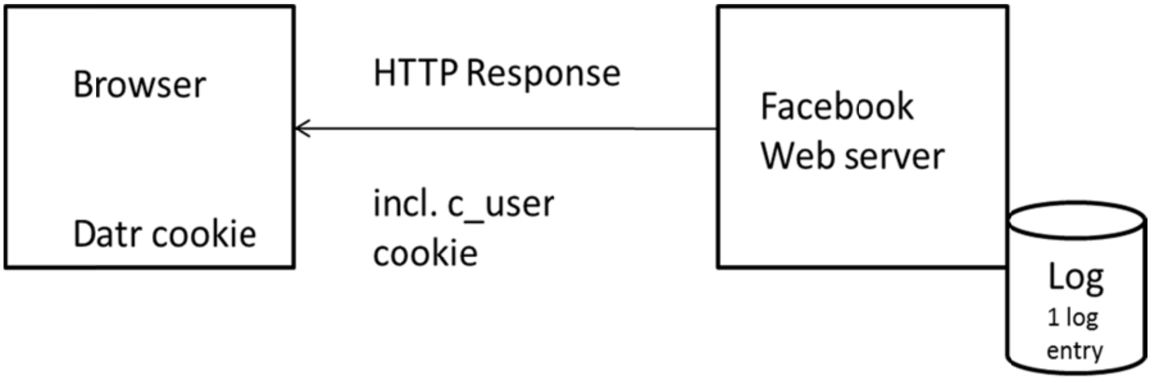
to keep track of all of the different browsers.

53. The Facebook server then responds by displaying a new webpage: the personal profile page of the new member.

54. After the user has entered their username and password and logged in, the server creates a new database entry. This new database entry corresponds to the actual user who logs in. Facebook uses a different large, random number to index into this database entry, e.g., 7890 (Small numbers are used here for illustration purposes. An actual index on Facebook is around 15 digits). The value 7890 is then sent in a new Set-Cookie header in the response to the browser. The browser stores this in a c_user cookie on the client machine in the cookie directory.

55. The datr cookie persists in the browser as well.

56. At the end of this interaction, the browser has the *c_user* cookie stored on the user's machine, and the Facebook server has an entry for that user, indexed by the value of that cookie.



B. Facebook's Tracking Of Logged-In Members

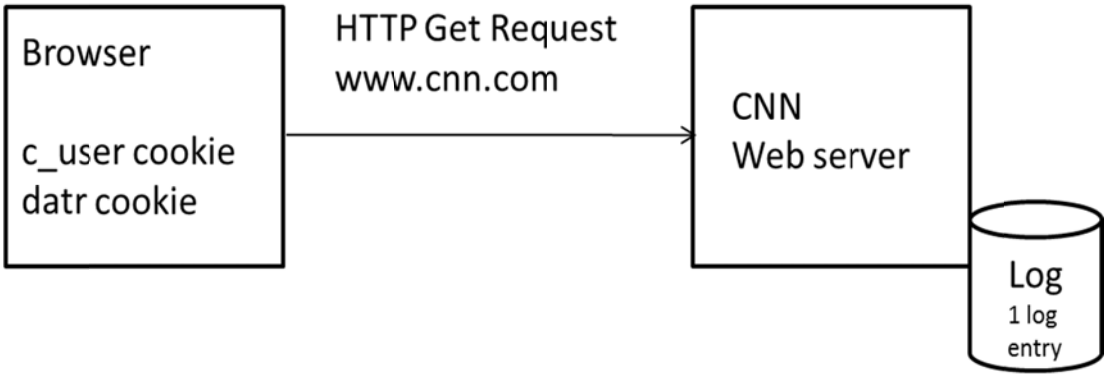
57. When a user visits another site on the internet that has any type of Facebook content integrated into the website, the Facebook.com server is notified of that electronic communication. That process occurs as follows:

58. The user visits another website by typing in a new URL (for example, www.cnn.com) in the browser address bar (CNN has Facebook content integrated into the site).

/ / /

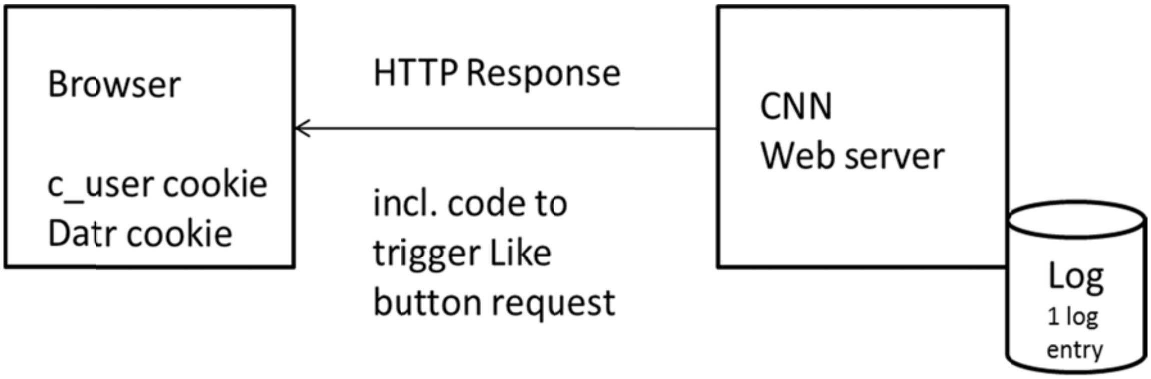
/ / /

59. The browser sends a GET request to the CNN server to display the webpage. If CNN had previously set any cookies on the browser, and they were not expired, then the browser would send those as well.



60. When the CNN server receives this request, it responds with the HTML file for the cnn.com home page. This HTML file contains information from third parties, who partner with CNN to display content on the CNN home page. For example, if a user sees a story that they like, they can click on the Facebook "Like" button, which is Facebook content embedded on the CNN website, and the story will show up in their Facebook news feed. To achieve this, CNN includes some special HTML code in the HTML for the web site.

61. Part of the contents of the response concern Facebook Like buttons. The CNN server does not send these button images, but instead sends a piece of code to the browser of the user:



62. The browser, triggered by the code, sends a request to the Facebook server to display the Like button. The HTML code on the CNN site looks like this: <a class="cnnShareFacebook"href="http://www.facebook.com/share.php?u=http%3A%2F%2Fwww.cnn.com%2F2012%2F05%2F15%2Fus%2Fsome-story-fbi%2Findex.html">Facebook</a>.

63. This is a tag that causes an automatic request to Facebook from the browser. The request includes the specific details of web page (or story) that the user has requested.

64. So, as a result of the user who is logged into Facebook requesting a story from CNN, the user's cookies, as well as the identity of the Web page that the user visited are sent to Facebook.

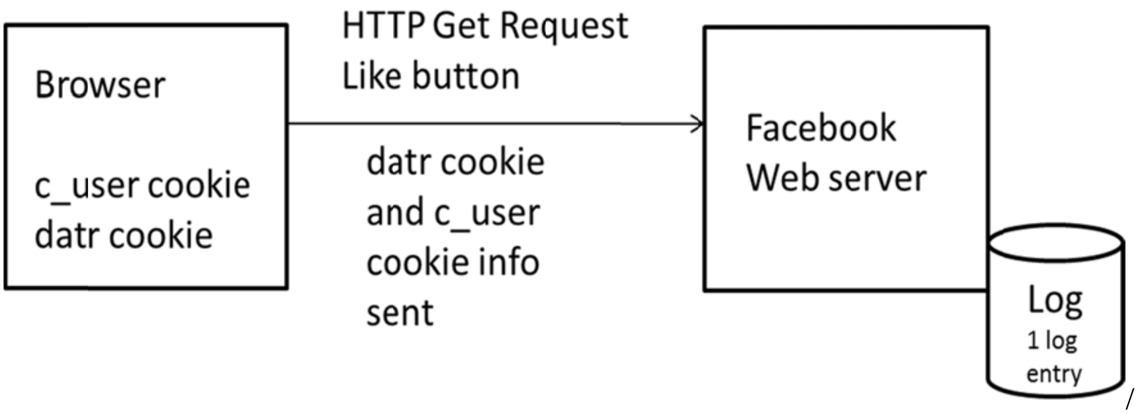
65. The request includes the information contained in the datr cookie.

66. The request includes the information contained in the c_user cookie.

67. When Facebook receives this information, it uses the 12345 and the 7890 indices to update its database records for the browser and the user, respectively, to add the information about which site the user visited, in this case, CNN.

68. Further, Facebook actually receives this information before the content of the user's request shows up on the user's screen. It is simultaneous with the request.

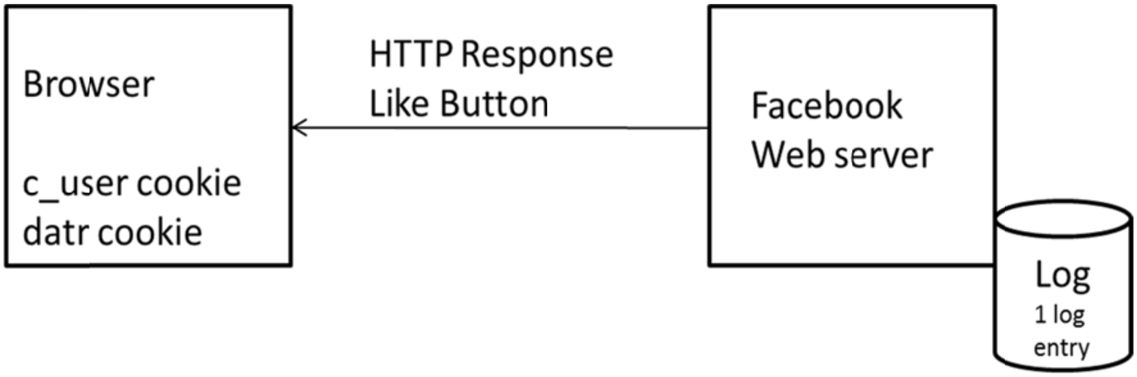
69. In a similar fashion, Facebook can keep track of all of the partner sites that users visit.



/ / /

/ / /

70. The Facebook server responds by sending the content which displays the Like button on the browser screen of the user (in the CNN website):

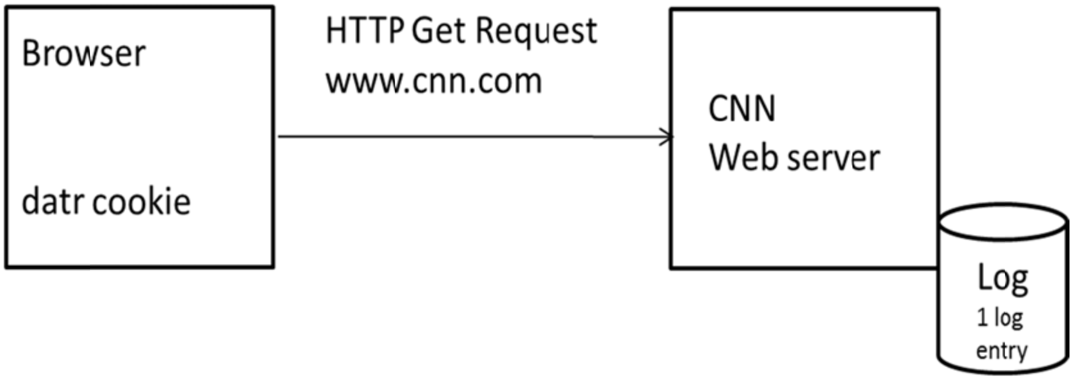


C. Facebook's Tracking Of Logged-Out Users

71. When a user logs out of Facebook, the Facebook.com server is still notified every time that user visits a website that has Facebook content integrated into the website. That process occurs as follows:

72. The user visits another website by typing in a new URL (www.cnn.com) in the browser address bar.

73. The browser sends a request to the CNN server to display the webpage:



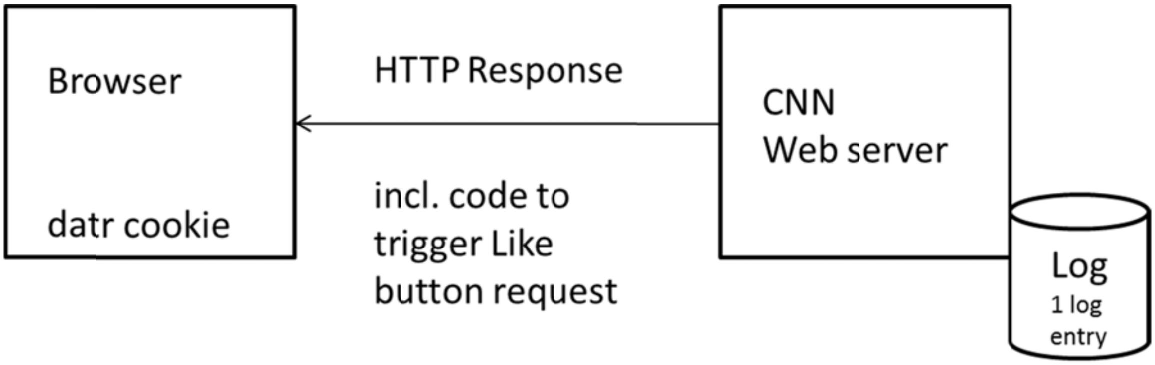
74. The CNN server responds by sending the contents of the webpage which are displayed on the browser screen of the user.

/ / /

/ / /

75. Part of the contents of the CNN web page concern Facebook Like buttons. The CNN server does not send these button images, but sends a piece of code to the browser of the user:

76.



77. The browser, triggered by the code, sends a request to the Facebook server to display the Like button.

78. The request includes information contained in cookies that contain personally identifiable information. By accessing this cookie information stored on the user's computer, Facebook has exceeded authorized access to the user's computer and intercepted an electronic communication because that cookie information was supposed to have been deleted upon log out.

79. Facebook creates a log entry of the request including the information from the cookies that contain personally identifiable information.

80. Facebook actually receives this information before the content of the user's request shows up on the user's screen. It is simultaneous with the request.

81. The Facebook server responds by sending the content which displays the Like button on the browser screen of the user.

/ / /

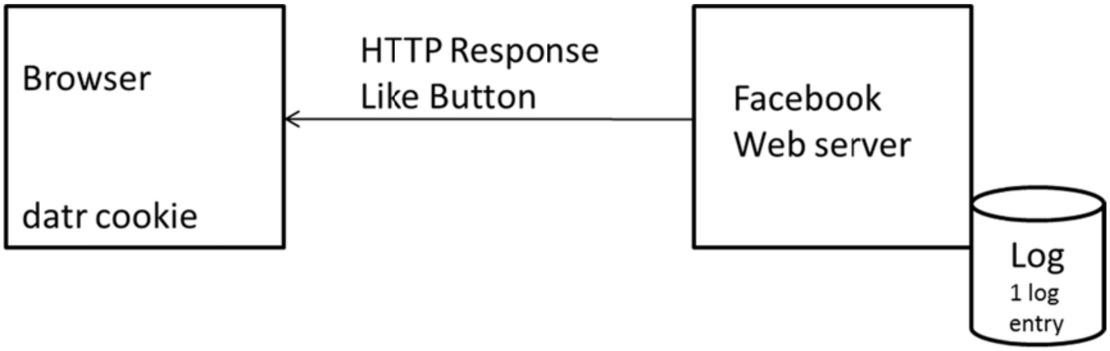
/ / /

/ / /

/ / /

/ / /

/ / /



82. Facebook's receipt of a copy of the user's request to the CNN server, along with the cookie information, is an interception of the contents of an electronic communication. By obtaining a duplicate copy of the user's communication with the website, Facebook obtains, in real time, the content of the datr tracking cookie and other persistent cookies, the details of that communication (which discloses what content exactly the user requested and constitutes a URL request), along with the date, time and web address of the webpages clicked on, the identification of the content accessed on each page, and the characteristics of the user's PC, mobile computer, cell phone and browser, such as the IP address, universal device identifier ("UDID") on mobile devices , screen resolution, operating system and browser version. All of this occurs while the user is logged off of Facebook, contrary to Facebook's governing policies.

83. Moreover, Facebook easily tracked logged out users with its datr tracking cookie alone, without the need for an additional Facebook cookie containing a Facebook user ID. From the first time a Facebook user logs into Facebook and the datr tracking cookie is set on his machine, all of that user's browsing to Facebook partner sites using that browser is linked by Facebook back to that user because the datr tracking cookie contains a unique number, which is also unique to that particular user's browser and his specific computer or mobile device, that indexes into the Facebook database which tracks users and browser sessions both on computers and mobile devices such as Android cell phones, iPhones, iPads and the iPod Touch.

84. Every time a user visits such a partner site, the datr tracking cookie with its unique number is sent to Facebook along with a duplicate of the same information as described above. Thus, in violation of the federal and California state laws enumerated below, Facebook used this information to track users after they logged out of Facebook.

III. FACEBOOK'S HISTORY AND PATTERN OF DISREGARD FOR THE PRIVACY RIGHTS OF ITS MEMBERS

85. Facebook has had a long history of disregard for the privacy rights of its members, including, but not limited to, the following:

1. May 2004: Zuckerberg hacked the personal email accounts of editors of the Harvard newspaper, utilizing private login information entered by users on Facebook's site;

2. Summer 2004: Zuckerberg hacked into a rival company's (ConnectU) networking site, purportedly for the purpose of disrupting the functionality of the program;

3. September 8, 2006: Zuckerberg acknwledges in a blog entry that "We really messed this one up. When we launched News Feed and Mini-Feed we were trying to provide you with a stream of information about your social world. Instead we did a bad job of explaining what the new features were and an even worse job of giving you control of them. I'd like to correct those errors now;"

4. August 2007: Configuration problem on Facebook's server allowed code to be displayed which put in doubt the privacy of Facebook users' personal information. Facebook responded, "A small fraction of the code that displays Facebook web pages was exposed to a small number of users due to a single misconfigured web server that was fixed immediately;"

5. November 2007: Blog post by Security Engineer at CA, Inc. claimed that Facebook Beacon was collecting data from affiliate sites even when users opted out and even when not logged into the site. There were concerns over Facebook utilizing this data and Facebook responded, "Facebook does not associate the information with any individual user account, and deletes the data as well;"

6. February 2008: Concerns arose that even when users close an account, Facebook could retain the information indefinitely. Facebook did not fix this problem until 2010;

7. May 2008: 35 page complaint by Canadian Internet Policy and Public Interest Clinic (CIPPIC) citing 22 breaches of Canadian law;

8. September 2009: Settlement of lawsuit over Beacon (shutting down the program);

9. December 2009: EPIC files lawsuit against Facebook regarding terms of service;

10. December 2009: FTC complaint against Facebook regarding the change to its privacy policies;

11. May 2010: “Quit Facebook Day” was a day set up where users would quit Facebook due to privacy concerns. 33,000 users quit that day;

12. December 2010: As of this date, 1,136 complaints had been filed with the Better Business Bureau;

13. August 2011: As of this date, 16 complaints had been filed against Facebook by the privacy rights advocacy group, Europe v. Facebook;

14. September 2011: Nik Cubrilovic discovers Facebook’s post log-out tracking;

15. November 2011: FTC settles complaint over Facebook Privacy issues by requiring extensive oversight. Zuckerberg responded, “I’m the first to admit that we’ve made a bunch of mistakes;” and

16. February 2012: Facebook was caught with the ability to read any text message sent over mobile phones and tablets which had downloaded its mobile app. Facebook responded that it uses this data for research and had only taken the texting inboxes of a handful of users.

IV. **FACEBOOK INTENTIONALLY CIRCUMVENTED WEB BROWSING PRIVACY P3P CODE IN ORDER TO TRACK USERS**

86. The Platform for Privacy Preferences (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.”[3]

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-

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

and four-letter tokens associated with P3P policy elements as defined in the P3P 1.0 Specification.4 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.”5 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

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

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

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

[5] P3P1.0 at Section 4.2.

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

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.[7]

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."[8]

93. IE treats 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 untruthful statements. Because of the way Microsoft implemented the P3P compact policy feature, websites can trick IE by simply leaving out any compact policy tokens that would lead IE6 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.

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."9 This report described a research study in which the

[7] Privacy in Microsoft Internet Explorer 6. October 2001. http://msdn.microsoft.com/en-us/library/ms537343

[8] Privacy in Microsoft Internet Explorer 6.

[9] http://www.cylab.cmu.edu/research/techreports/2010/tr_cylab10014.html.

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:[10]

> 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 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:

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

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

101. Facebook’s new compact policy still tricks IE into allowing Facebook’s cookies. Although the body of Facebook’s compact policy is an English-language statement, readable to humans, that indicates that Facebook does not actually have a P3P policy; compact policies are designed to be read by computers, not humans. The IE web browser does not have the ability to glean meaning from this English-language statement. All IE does is scan the words within this statement to see whether any of them are on its list of unsatisfactory P3P tokens. Since none of these words are unsatisfactory P3P tokens, IE is tricked into classifying the policy as satisfactory and allows the Facebook cookie.

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

V. **PLAINTIFFS’ SPECIFIC FACTUAL ALLEGATIONS**

103. Plaintiff Davis is a Facebook user and during the Class Period had an active Facebook account. Plaintiff Davis, using the same computer on which Facebook installed tracking and session cookies, visited websites with Facebook-integrated content after logging out of her Facebook account. Contrary to its policies, Facebook intercepted Plaintiff Davis’ electronic communications and tracked her internet use post-logout. Plaintiff did not consent to post-logout tracking.

104. Plaintiff Quinn is a Facebook user and during the Class Period had an active Facebook account. Plaintiff Quinn, using the same computer on which Facebook installed tracking and session cookies, visited websites with Facebook integrated content after logging out of her Facebook account. Contrary to its policies, Facebook intercepted Plaintiff Quinn’s electronic communications and tracked her internet use post-logout. Plaintiff did not consent to post-logout tracking.

105. Plaintiff Lentz is a Facebook user and during the Class Period had an active Facebook account. Plaintiff Lentz, using the same computer on which Facebook installed tracking and session cookies, visited websites with Facebook integrated content after logging out of his Facebook account. Contrary to its policies, Facebook intercepted Plaintiff Lentz’s electronic

communications and tracked his internet use post-logout. Plaintiff did not consent to post-logout tracking.

106. Plaintiff Vickery is a Facebook user and during the Class Period had an active Facebook account. Plaintiff Vickery, using the same computer on which Facebook installed tracking and session cookies, visited websites with Facebook integrated content after logging out of his Facebook account. Contrary to its policies, Facebook intercepted Plaintiff Vickery's electronic communications and tracked his internet use post-logout. Plaintiff did not consent to post-logout tracking.

107. The Wiretap Act, as discussed in more detail below, provides statutory damages of the greater of $100 per violation per day, up to $10,000, per Facebook user.

108. Plaintiffs are thus each entitled to the greater of $100 of statutory damages per day (corresponding to $15 billion for the Class), or $10,000 each for the ongoing violations during the class period (corresponding to $1.5 trillion for the Class).

109. Plaintiff Davis, through counsel, also retained a computer and computer law expert to advise her and counsel on the nature of Facebook's violations, the technologies and remedies. The expert was paid a retainer of $7,500.

110. The Computer Fraud and Abuse Act, as discussed in more detail below, statutorily provides for reimbursement of out-of-pocket costs incurred as a result of Defendant's violations of the Act if such costs exceed $5,000. Plaintiff Davis is thus entitled to reimbursement of these damages as are any other Class Members who incurred out-of-pocket costs as a result of Defendant's violations.

VI. <u>THEFT OF PERSONALLY IDENTIFIABLE INFORMATION</u>

111. Facebook admits that users must "provide their name, age, gender, and a valid email address, and agree to Facebook's terms of service."

112. Although Facebook members are not required to transmit cash to Facebook, the personal information Facebook requires has massive economic value. More importantly, Facebook conditioned membership upon the user accepting numerous Facebook cookies, which track

browsing history, on the user's computer. This browsing history has even greater economic value.

113. The value of the information that users are required to provide to Facebook is well understood in the e-commerce industry, and personal information is now viewed as a form of currency.

114. 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.

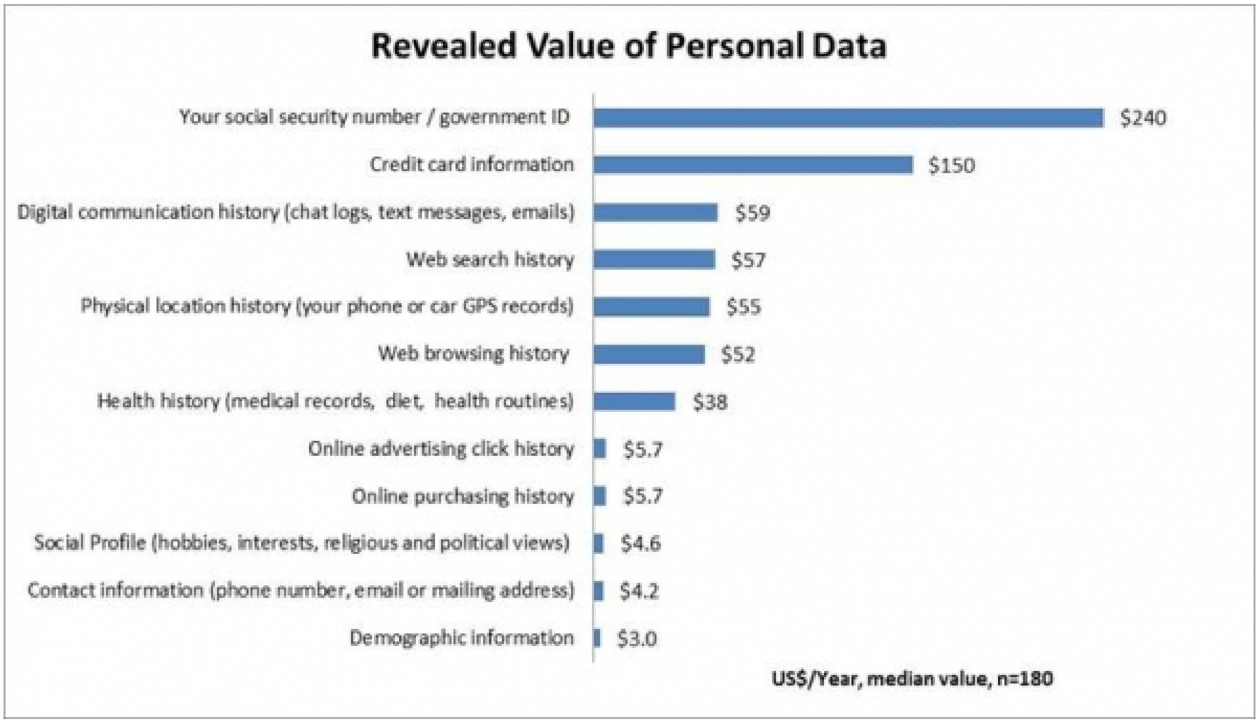
115. Likewise, in the Wall Street Journal, privacy expert and fellow at the Open Society Institute Christopher Soghoian noted:

> 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).

116. The cash value of users' personal information provided to Facebook as a condition of membership can be quantified. For example, in a recent study authored by Tim Morey ("What's Your Personal Data Worth? http://designmind.frogdesign.com/blog/what039s-your-personal-data-worth.html, Jan. 18, 2011), researchers studied the value that 180 internet users

placed on keeping personal data secure. The results were striking. 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. 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, these figures imply aggregate annual membership fees of $3.36 billion, $2.4 billion, and $41.6 billion, respectively, for each category of information.

117. Similarly, the value of personal data and internet browsing history can be quantified, because at least two internet giants are willing to pay users for the exact type of data that Facebook illegally intercepted from Plaintiffs and other members of the Class.

118. For example, Google Inc. now has a panel called "Google Screenwise Trends" which, according to the internet giant, is designed "to learn more about how everyday people use the Intenet."

119. Upon becoming a panelist, internet users add a browser extension that will share with Google the sites that users visit and how the panelist uses them. The panelist consents 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.

120. After three months, Google also agrees to pay panelists additional unspecified gifts “for staying with” the panel.

121. These gift cards, mostly valued at exactly $5, demonstrate conclusively that internet industry participants now generally understand 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 that the industry is starting to settle on a rough consensus as to the value of the information harvested by Facebook.

122. Moreover, active markets exist all over the world for this type of data. For instance, a company in the United Kingdom, Allow Ltd., has created a business model based on the value of personally identifiable information. When a customer signs up for Allow ltd., the company sends a letter on behalf of their new client to the top companies in the United Kingdom that harvest personal data demanding that those companies immediately stop using the client’s personally identifiable data.

123. Because that data is not readily available, it becomes highly coveted by advertisers, and thus, applying basic economic principles, its value as a commodity increases in the market. In contrast, the more accessible the user’s data, the less valuable it becomes on the open market.

124. United States data markets work the same way. The more a person’s personally identifiable data is used, the less money someone will pay for it. Consequently, an individual’s personally identifiable data diminishes in value each time that data is intercepted and then sold to advertisers, data aggregators and other third parties without the individual’s consent.

125. In the instant case, Facebook intentionally intercepted Plaintiffs’ personally identifiable data without consent. Thus, in addition to the concrete and quantifiable damages described above, Plaintiffs have also suffered damages as a result of the decreased value of their data in the marketplace.

VII. <u>ADDITIONAL CONSEQUENTIAL DAMAGES</u>

126. Plaintiff Davis signed up for a service called “Privacy Watch” from Abine, an online privacy company.

127. Privacy Watch is an email alert service specifically targeted at Facebook. Subcribers receive alerts when Facebook changes its Data Use Policy or makes changes to privacy controls and provides expert assistance for Facebook users looking to protect their privacy.

128. The Privacy Watch service costs $1.99 per month, or approximately $24 per year.

129. Plaintiff Davis subscribed to the service and incurred this expense as a direct result of Facebook's failure during the Class Period to abide by its privacy policies.

VIII. <u>FACEBOOK TRACKED ITS MEMBERS' POST-LOGOUT INTERNET USE INTENTIONALLY</u>

130. As set forth in detail herein, Facebook's intentional interception of members' electronic communications, including their internet browsing activity, coupled with their personally identifiable data, without consent, even after logging out of Facebook, is evidenced by the following:

(1) Facebook's Patent Application, which demonstrates that Facebook employed technology specifically designed to track users while logged out;

(2) Facebook's contradictory responses to regulators, including claims that the persistence of certain cookies post-log-out was both a "bug" and that Facebook "needs" personally identifiable information after log-out in order to guarantee security;

(3) The report issued by German authorities, explaining that Facebook's alleged reasons for "needing" personal information after log-out were "untenable";

(4) Facebook's pervasive violations of individual privacy;

(5) The use of different cookies to track users prior to and post log-out, in addition to cookies that track non-Facebook members;

(6) Facebook's knowledge of the tracking issue at least a year prior to its admission that it needed to correct this "bug" based on the findings of Nic

Cubrilovic, who repeatedly contacted the Company, but received no response until he posted the information on his blog; and

(7) Facebook's use of the P3P tracking cookie.

CLASS ACTION ALLEGATIONS

131. 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 May 27, 2010 and September 26, 2011, both dates inclusive, and whose privacy Facebook violated. Excluded from the Class are 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.

132. The members of the Class are so numerous that joinder of all members is impracticable.

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

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

135. Plaintiffs will fairly and adequately protect the interests of the members of the Class 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 members.

136. 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 members have suffered may be relatively small, the expense and burden

of individual litigation make it impossible for members of the Class to individually redress the wrongs done to them. There will be no difficulty in management of this action as a class action.

COUNT I

VIOLATION OF THE FEDERAL WIRETAP ACT, 18 U.S.C. § 2510, *et. seq.*

137. Plaintiffs incorporate the above allegations by reference as if set forth more fully herein.

138. The Federal Wiretap Act, as amended by the Electronic Communications Privacy Act of 1986, prohibits the intentional interception of any wire, oral, or electronic communication.

139. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire, oral or electronic communication is intercepted.

140. Facebook intercepted the contents of Plaintiffs' and Class Members' electronic communications even after such users had logged out of Facebook, contrary to its governing policies and without the consent of its users.

141. Neither the Plaintiffs nor members of the Class were aware that Facebook was violating its own privacy policy, intercepting its users' electronic communications and tracking their detailed web browsing habits after users logged out of Facebook.

142. By duplicating its users' communications with websites that use Facebook content (the users' URL requests for information) and associating it with cookies and other data, Facebook used technology to acquire the contents of those electronic communications within the meaning of the Wiretap Act.

143. Facebook intentionally made copies of such detailed website requests and personally identifiable information using a device on users' computers, its web servers and technology, and thus intentionally intercepted the electronic communications of its users.

144. Plaintiffs and Class Members are persons whose electronic communications were intercepted within the meaning of Section 2520.

145. Section 2520 provides for preliminary, equitable and declaratory relief, in addition to statutory damages of the greater of $10,000 or $100 a day for each day of violation or actual damages, punitive damages in appropriate cases, reasonable attorneys' fees, and other litigation

costs reasonably incurred.

COUNT II

VIOLATION OF THE STORED COMMUNICATIONS ACT, 18 U.S.C. § 2701, et. seq.

146. Plaintiffs incorporate the above allegations by reference as if set forth more fully herein.

147. 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.

148. The statute 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."

149. Facebook's access of persistent cookies on Plaintiffs' and Class Members' computers without their consent and in violation it privacy policies after logout from Facebook exceeded authorized access to those computers, which are facilities through which an electronic communication service is provided. By using technology that caused cookie data to be sent to Facebook without Plaintiffs' or Class Members' consent or knowledge, Facebook obtained electronic communication data in electronic storage in violation of the SCA.

150. Plaintiffs and other member of the Class were harmed by Defendant's violations, and pursuant to 18 U.S.C. § 2707(c), are entitled to actual damages including profits earned by Defendant attributable to the violations or statutory minimum damages of $1,000 per person, punitive damages, costs and reasonable attorneys' fees.

/ / /

/ / /

/ / /

COUNT III

VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT, 18 U.S.C. § 1030

151. Plaintiffs incorporate the above allegations by reference as if set forth more fully herein.

152. Plaintiffs' and Class Members' computers were used in interstate commerce or communication.

153. Defendant intentionally accessed Plaintiffs' and Class Members computers without authorization or by exceeding authorized access to such computers, and by obtaining information from such a protected computers.

154. Defendant knowingly caused the transmission of a program, information, code or command to said computers and as a result caused a loss to Plaintiffs and Class Members during any one-year period of at least $5,000 in the aggregate.

155. Plaintiffs and Class Members have also suffered a violation of the right of privacy as a result of Defendant's knowing actions.

156. Defendant has thus violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

157. Defendant's unlawful access to Plaintiffs' and Class Members' computers and communications have caused irreparable injury. Unless restrained and enjoined, Defendant will continue to commit such acts. Plaintiffs' and Class Members' remedies at law are not adequate to compensate for these inflicted and threatened injuries, entitling Plaintiffs and the Class to remedies including injunctive relief as provided by 18 U.S.C. § 1030(g).

COUNT IV

INVASION OF PRIVACY

158. Plaintiffs incorporate all preceding paragraphs as though fully set forth herein.

159. Plaintiffs had an interest in: (1) precluding the dissemination and/or misuse of their sensitive, confidential personally identifiable information; and (2) making personal decisions and/or conducting personal activities without observation, intrusion or interference, including, but not limited to, the right to visit and interact with various internet sites without having that

information intercepted and transmitted to Defendant without their knowledge or consent.

160. Based on, among other things, Facebook's Terms of Use and Privacy Policy, Plaintiffs had a reasonable expectation that their personally identifiable information and other data would remain confidential and that Defendant would not install cookies on their browsers that would enable Facebook to track their activities on the internet after logging out of their Facebook accounts.

161. This invasion of privacy is sufficiently serious in nature, scope and impact.

162. This invasion of privacy constitutes an egregious breach of the social norms underlying the privacy right.

COUNT V

INTRUSION UPON SECLUSION

163. Plaintiffs incorporate all preceding paragraphs as though fully set forth herein.

164. By intercepting Plaintiffs' wire and electronic communications on the internet, Defendants intentionally intruded upon their solitude or seclusion.

165. Plaintiffs did not consent to Defendants' intrusion.

166. Defendants' intentional intrusion on Plaintiffs' solitude or seclusion without consent would be highly offensive to a reasonable person.

COUNT VI

CONVERSION

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

168. Plaintiffs and the Class Members own and/or have a right to possess their personally identifiable information and other data, including, but not limited to, their names, account information, browsing histories, and purchasing habits. Such property, owned by Plaintiffs and the Class Members, is valuable to Plaintiffs and the Class Members.

169. Defendant unlawfully exercised dominion over said property and thereby converted Plaintiffs' and the Class Members' property, by, inter alia, installing cookies on Plaintiffs' and the Class Members' computers, which continued to intercept their communications after they were

logged out of their Facebook accounts.

170. Plaintiffs and the Class Members have suffered damages as a result of Defendant's actions, including, but not limited to, the loss in value of their personally identifiable information in the marketplace.

COUNT VII

TRESPASS TO CHATTELS

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

172. Defendant, intentionally and without consent or other legal justification, tracked Plaintiffs' activity while Plaintiffs were logged-off of the website Facebook.com, and, in the process, connected Plaintiffs' personally identifiable information to their specific actions on the Internet.

173. Defendant, intentionally and without consent or other legal justification, placed cookies on Plaintiffs' computers which tracked their activity while logged-off of Facebook.

174. 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 VIII

VIOLATION OF CALIFORNIA BUSINESS AND PROFESSIONAL CODE § 17200, ET SEQ., THE UNFAIR COMPETITION LAW ("UCL")

175. Plaintiffs incorporate all preceding paragraphs a though set forth herein.

176. In violation of California Business and Professional Code § 17200, et seq., Defendant's conduct in this regard is ongoing and includes, but is not limited to, statements made by Defendant in its information privacy and confidentiality practices.

177. By engaging in the acts and practices described herein, Defendant has committed one or more acts of unfair competition within the meaning of the UCL, and as a result, Plaintiffs and the Class Members have suffered injury-in-fact and have lost money and/or property, namely, as described herein, the insertion of cookies on their computers and the invasion and lost value of

their personally identifiable information and other data.

178. In reasonable reliance on Defendant’s misrepresentations and omissions, Plaintiffs interacted with various websites while logged out of their Facebook accounts believing that this information was secure and confidential. In actuality, without Plaintiffs’ knowledge or consent, Defendant caused certain cookies to be placed on Plaintiffs’ computers, which actively intercepted and collected Plaintiffs’ personally identifiable information so that it could be utilized for advertising and other purposes for Defendant’s benefit.

179. Defendant’s business acts and practices are unlawful, in part, because they violate California Business and Professions Code§ 17500, et seq., which prohibits false advertising, in that they were untrue and misleading statements relating to Defendant’s performance of services, made with the intent to induce consumers to enter into obligations relating to such services, and regarding which statements Defendant knew, or which by the exercise of reasonable care Defendant should have known, to be untrue and misleading. Defendant’s business acts and practices are also unlawful in that they violate the California Consumers Legal Remedies Act, California Civil Code § 1750, et seq., California Penal Code § 502, California Penal Code §630, 18 U.S.C. § 2511, et seq., and 18 U.S.C. § 1030. Defendant is therefore in violation of the “unlawful” prong of the UCL.

180. Defendant’s business acts and practices are unfair, because they cause harm and injury in fact to Plaintiffs and Class Members, and for which Defendant has no justification other than to increase, beyond what Defendant would have otherwise realized, its profit in fees from advertisers, software developers and other third parties and the value of its information assets through the acquisition of consumers’ personal information. Defendant’s conduct lacks reasonable and legitimate justification in that Defendant has benefited from such conduct and practices while Plaintiffs and the Class Members have been misled as to the nature and integrity of Defendant’s services and have, in fact, suffered material disadvantage regarding their interests in the privacy and confidentiality of their personal information. Defendant’s conduct offends public policy in California as embodied in the Consumers Legal Remedies Act, the state constitutional right of privacy, and California statutes recognizing the need for consumers to obtain material

information that enables them safeguard their own privacy interests, including Cal. Civ. Code § 1798.80.

181. Moreover, Defendant knew, or should have known, that consumers care about the status of personal information and internet privacy, but are unlikely to be aware of the manner in which Defendant was engaged in practices that expressly violated its stated Privacy Policy and the Terms of Use. Defendant therefore is in violation of the "unfair" prong of the UCL.

182. Defendant's acts and practices were fraudulent within the meaning of the UCL, because they were likely to, and did, in fact, mislead the members of the public to whom they were directed.

183. Plaintiffs, on behalf of themselves and each Class Member, seek restitution, injunctive relief, and other relief as provided under the UCL.

COUNT IX

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

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

185. 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.

186. 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.

187. 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."

/ / /

188. 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.

189. 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.

190. 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.

191. 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."

192. Defendants have violated California Penal Code § 502(6)(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.

193. 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).

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

195. Plaintiff and Class Members have suffered irreparable and incalculable harm and injuries from Defendant's violations. The harm will continue unless Defendant is enjoined from

further violations of this section. Plaintiffs and Class Members have no adequate remedy at law.

196. 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.

197. Plaintiffs and the Class Members have also suffered irreparable injury from these unauthorized acts of disclosure, to wit: all of their personal, private, and sensitive web communications have been harvested, viewed, accessed, stored, and used by Defendant, and have not been destroyed, and due to the continuing threat of such injury, have no adequate remedy at law, entitling Plaintiffs to injunctive relief.

COUNT X

VIOLATIONS OF CALIFORNIA PENAL CODE § 630
THE INVASION OF PRIVACY ACT

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

199. California Penal Code § 631(a) provides, in pertinent part:

> Any person who … 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…

200. At all relevant times, Defendant’s business practice of depositing a cookie that continued to access, intercept and collect Plaintiffs’ and Class Members’ personally identifiable information and other data, including information concerning their interactions with certain websites, after log-out from Facebook.com was without authorization and consent, including, but not limited to, obtaining any and all communications.

/ / /

201. Upon information and belief, Plaintiffs, and each Class Member, during one or more of their interactions on the internet during the Class Period, communicated with one or more entities based in California, or with one or more entities whose servers were located in California.

202. Communications from the California web-based entities to Plaintiffs and Class Members were sent from California. Communications to the California web-based entities from Plaintiffs and Class Members were sent to California.

203. Plaintiffs and Class Members did not consent to any of Defendant's actions in intercepting, reading, and/or learning the contents of their communications with such California-based entities.

204. Plaintiff and Class Members did not consent to any of the Defendant's actions in using the contents of their communications with such California-based entities.

205. Defendant is not a "public utility engaged in the business of providing communications services and facilities..."

206. The actions alleged herein by Defendant was not undertaken "for the purpose of construction, maintenance, conduct or operation of the services and facilities of the public utility."

207. The actions alleged herein by Defendant was not undertaken with respect to any telephonic communication system used for communication exclusively within a state, county, city and county, or city correctional facility.

208. Defendant directly participated in the interception, reading, and/or learning of the contents of the communications between Plaintiffs, Class Members and California-based web entities.

209. Plaintiffs and Class Members have additionally suffered loss by reason of these violations, including, without limitation, violation of the right of privacy and deprivation of the loss of value in their personally identifiable information.

210. Unless restrained and enjoined, Defendants will continue to commit such acts.

211. Pursuant to Section 637.2 of the California Penal Code, Plaintiff and the Class have been injured by the violations of California Penal Code § 631. Wherefore, Plaintiffs, on behalf of themselves and on behalf of a similarly situated Class of consumers, seeks damages and injunctive

relief.

COUNT XI

VIOLATIONS OF CALIFORNIA CIVIL CODE § 1750
THE CONSUMER LEGAL REMEDIES ACT

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

213. In violation of California Civil Code § 1750, et seq. (the "CLRA"), Defendant has engaged and is engaged in unfair and deceptive acts and practices in the course of its interactions with Plaintiffs and Class Members.

214. At all relevant times, Plaintiffs and each proposed Class Member was a "consumer," as that term is defined in Civ. Code § 1761(d).

215. At all relevant times, Defendant's online services constituted "services," as that term is defined in Civ. Code § 1761(b).

216. At all relevant times, Defendant was a "person," as that term is defined in Civ. Code § 1761(c).

217. At all relevant times, Plaintiffs' and each proposed Class Member's use of Defendant's website and the implementation of cookies constituted a "transaction," as that term is defined in Civ. Code § 1761(e).

218. Defendant's practices, acts, policies, and course of conduct violated the CLRA in that Defendant represented that its website and online services have characteristics, uses and benefits which they do not have, in violation of § 1770(a)(5) of the CLRA.

219. Defendant's practices, acts, policies, and course of conduct violated the CLRA in that Defendant represented that a transaction confers or involves rights, remedies, or obligations which it does not have, in violation of § 1770(a)(14) of the CLRA.

220. As previously described in detail, Defendant represented that it would supply its service to Plaintiffs and Class Members in accordance with the governing documents and then did not, in violation of § 1770(a)(16).

221. Plaintiffs and the Class relied on Defendant's representations that it would supply its service in accordance with the governing documents.

222. Plaintiffs and the Class suffered the aforementioned damages as a result of the Defendant's conduct.

223. Plaintiffs seek only injunctive relief for the CLRA claims alleged in this Complaint.

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.

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

JURY TRIAL DEMAND

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

DATED this 17th day of May, 2012.

Respectfully submitted,

BARTIMUS, FRICKLETON,
ROBERTSON & GORNY, P.C.

/s/ *Edward D. Robertson Jr.*
Edward D. Robertson, Jr.
James P. Frickleton
Mary D. Winter
Edward D. Robertson III
11150 Overbrook Road, Suite 200
Leawood, KS 66211
chiprob@earthlink.net
Telephone: (913) 266-2300
Facsimile: (913) 266-2366
Interim Co-Lead Counsel

STEWARTS LAW US LLP

/s/ David A. Straite
David A. Straite (admitted *pro hac vice*)
Ralph N. Sianni
Michele S. Carino
Lydia E. York
1201 North Orange Street, Suite 740
Wilmington, DE 19801
dstraite@stewartslaw.com
Telephone: (302) 298-1200
Facsimile: (302) 298-1222
Interim Co-Lead Counsel

KIESEL BOUCHER LARSON LLP
Paul R. Kiesel, Esq. (SBN 119854)
8648 Wilshire Boulevard
Beverly Hills, CA 90211
kiesel@kbla.com
Telephone: (310) 854-4444
Facsimile: (310) 854-0812
Interim Liaison Counsel

Stephen G. Grygiel
John E. Keefe, Jr.
Jennifer Harwood
KEEFE BARTELS LLC
170 Monmouth Street
Red Bank, NJ 07701
Telephone: (732) 224-9400
Facsimile: (732) 224-9494
sgrygiel@keefebartels.com
Plaintiffs' Steering Committee Member

Michael S. Schwartz
Mark S. Mandell
Zachary Mandell
MANDELL, SCHWARTZ & BOISCLAIR, LTD.
1 Park Row
Providence, RI 02903
msmandell@msb-atty.com
Telephone: (401) 273-8330
Facsimile: (401) 751-7830
Plaintiffs' Steering Committee Member

Barry R. Eichen
Daryl L. Zaslow
Tom Paciorkowski
EICHEN CRUTCHLOW ZASLOW &
MCELROY LLP
40 Ethel Road
Edison, New Jersey 08817
Telephone: (732) 777-0100

Stephen M. Gorny
BARTIMUS, FRICKLETON,
ROBERTSON & GORNY, P.C.
11150 Overbrook Road, Suite 200
Leawood, KS 66211
steve@bflawfirm.com
Telephone: (913) 266-2300
Facsimile: (913) 266-2366

Facsimile: (732) 248-8273
beichen@njadvocates.com
Plaintiffs' Steering Committee Member

Plaintiffs' Steering Committee Member

Andrew J. Lyskowski
Erik A. Bergmanis
BERGMANIS LAW FIRM, L.L.C.
380 W. Hwy. 54, Suite 201
P.O. Box 229
Camdenton, MO 65020
alyskowski@ozarklawcenter.com
Telephone: (573) 346-2111
Facsimile: (573) 346-5885
Plaintiffs' Steering Committee Member

William M. Cunningham, Jr.
Peter S. Mackey
Peter F. Burns
BURNS CUNNINGHAM & MACKEY PC
P.O. Box 1583
Mobile, AL 36633
wmcunningham@bcmlawyers.com
Telephone: (251) 432-0612
Facsimile: (251) 432-0625
Plaintiffs' Steering Committee Member

William H. Murphy, Jr.
William H. Murphy, III
Tonya Osborne Baña
MURPHY, FALCON & MURPHY, P.A.
One South Street, 23rd Floor
Baltimore, MD 21202
billy.murphy@murphypa.com
Telephone: (410) 539-6500
Facsimile: (410) 539-6599
Plaintiffs' Steering Committee Member

Margery S. Bronster
Robert Hatch
BRONSTER HOSHIBATA
1003 Bishop Street, Suite 2300
Honolulu, Hawaii 96813
mbronster@bhhawaii.net
Telephone: (808) 524-5644
Facsimile: (808) 599-1881
Special State AG Advisory Committee Member

Richard P. Ieyoub
Michael Reese Davis
L. J. Hymel
Tim P. Hartdegen
HYMEL, DAVIS & PETERSEN, LLC
10602 Coursey Blvd.
Baton Rouge, LA 70816
rieyoub@hymeldavis.com
Telephone: (225) 298-8188
Facsimile: (225) 298-8119
Special State AG Advisory Committee Member

Grant Woods
GRANT WOODS PC
Two Renaissance Square
40 N. Central Ave., Suite 2250
Phoenix, AZ 85004
gw@grantwoodspc.net
Telephone: (602) 258-2599
Facsimile: (602) 258-5070
Special State AG Advisory Committee Member

Mike Moore
MIKE MOORE LAW FIRM, LLC
10 Canebrake Blvd.
Suite 150 Flowood, MS 39232
mm@mikemoorelawfirm.com
Telephone: (601) 933-0070
Facsimile: (601) 933-0071
Special State AG Advisory Committee Member

CERTIFICATE OF SERVICE

I hereby certify that on May 17, 2012, 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 May 17, 2012.

DATED: May 17, 2012

Respectfully Submitted,

KIESEL BOUCHER LARSON 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