

1 Michael W. Sobol (State Bar No. 194857)
msobol@lchb.com
2 Melissa Gardner (State Bar No. 289096)
mgardner@lchb.com
3 LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
275 Battery Street, 29th Floor
4 San Francisco, CA 94111-3339
Telephone: 415.956.1000
5 Facsimile: 415.956.1008

6 Rachel Geman
rgeman@lchb.com
7 Nicholas Diamand
ndiamand@lchb.com
8 LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
250 Hudson Street, 8th Floor
9 New York, NY 10013-1413
Telephone: 212.355.9500
10 Facsimile: 212.355.9592

11 Hank Bates (State Bar No. 167688)
hbates@cbplaw.com
12 Allen Carney
acarney@cbplaw.com
13 David Slade
dslade@cbplaw.com
14 CARNEY BATES & PULLIAM, PLLC
11311 Arcade Drive
15 Little Rock, AR 72212
Telephone: 501.312.8500
16 Facsimile: 501.312.8505

17 *Attorneys for Plaintiffs*

18 UNITED STATES DISTRICT COURT
19
20 NORTHERN DISTRICT OF CALIFORNIA

21 MATTHEW CAMPBELL and MICHAEL
22 HURLEY, on behalf of themselves and all
23 others similarly situated,

24 Plaintiffs,

25 v.

26 FACEBOOK, INC.,

27 Defendant.
28

Case No. _____

CLASS ACTION COMPLAINT

CLASS ACTION COMPLAINT

I. INTRODUCTION

1. The right of privacy is a personal and fundamental right in California¹ and the United States.² An individual's privacy is directly implicated by the collection, use, and dissemination of personal information. Defendant Facebook, Inc. ("Facebook" or "the Company") has systematically violated consumers' privacy by reading its users' personal, private Facebook messages without their consent.

2. Facebook is a social-networking site that boasts more than one billion users worldwide, making it the largest online social network in the world.

3. Across the various services it offers, Facebook takes pains to promise a stark distinction in the types of communications it facilitates. Users may choose to communicate publicly via individual Facebook pages, or privately via personal messages and chats.³

4. Specifically, Facebook describes communication options "[d]epending on whom you'd like to share with." The options range from the broadest possible audience (a post which the public may see, including via searches on the internet), to posts viewable by small groups of friends, to Facebook messages shared "privately" with a single individual.⁴ Facebook touts the privacy of its messaging function as "unprecedented" in terms of user control and the prevention of unwanted contact.⁵

¹ CAL. CONST., Art. I, § 1, adopted as ballot measure in 1972 ("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."). See also *Am. Acad. of Pediatrics v. Lungren*, 16 Cal. 4th 307, 326 (1997) ("[T]he scope and application of the state constitutional right of privacy is broader and more protective of privacy than the federal constitutional right of privacy as interpreted by the federal courts.").

² *Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 763 (1989) ("both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person"); *Whalen v. Roe*, 429 U.S. 589, 605 (1977).

³ The distinction between "messages" and "chats" on Facebook is one of timing: chats happen in real-time and often give the appearance of conversation, whereas messages act more like email.

⁴ *Help Center: Get Started on Facebook: How to Post & Share*, Facebook, <https://www.facebook.com/help/333140160100643/>.

⁵ Joel Seligstein, *See the Messages that Matter*, Facebook, <https://www.facebook.com/notes/facebook/see-the-messages-that-matter/452288242130>.

1 5. Contrary to its representations, “private” Facebook messages are systematically
2 intercepted by the Company in an effort to learn the contents of the users’ communications. In
3 the course of the last year, independent security researchers discovered that Facebook reviews the
4 contents of its users’ private Facebook messages for purposes unrelated to the facilitation of
5 message transmission. When a user composes a Facebook message and includes a link to a third
6 party website (a “URL”)⁶, the Company scans the content of the Facebook message, follows the
7 enclosed link, and searches for information to profile the message-sender’s web activity.

8 6. This practice is not done to facilitate the transmission of users’ communications
9 via Facebook, but because it enables Facebook to mine user data and profit from those data by
10 sharing them with third parties – namely, advertisers, marketers, and other data aggregators.

11 7. Representing to users that the content of Facebook messages is “private” creates
12 an especially profitable opportunity for Facebook, because users who believe they are
13 communicating on a service free from surveillance are likely to reveal facts about themselves that
14 they would not reveal had they known the content was being monitored. Thus, Facebook has
15 positioned itself to acquire pieces of the users’ profiles that are likely unavailable to other data
16 aggregators.

17 8. Almost the entirety of Facebook’s revenues derive from the sale of third party
18 advertisements, which the Company is able to target towards its users based upon the personal
19 data it mines and stores. In 2011, Facebook earned \$2.7 billion from targeted advertising sales.
20 The more otherwise-unavailable information the Company can collect about its users – including
21 the contents of their private communications – the more valuable its advertising capacity.
22 Accordingly, Facebook promotes itself as a rich source of information about the people who use
23 the site, one which allows businesses to “reach the right people,” through selective targeting of
24
25
26

27 ⁶ A “URL,” or “uniform resource locator” is also known as a “web address.” It is a character
28 string that refers to a specific resource or location on the Internet. For example,
“www.nytimes.com” is the URL for the *New York Times*’ home page.

1 potential customers by, for example, “location,” “age,” or “interests”⁷ drawn from “activities,
2 education, job titles, Pages they like or groups to which they belong.”⁸

3 9. All of Facebook’s activities complained of herein are performed without users’
4 consent. Instead, to increase users’ comfort with the website and, thereby, increase the amount of
5 information they share, the Company makes assurances of user control over privacy settings and
6 messaging options. These assurances affirmatively state that only senders and intended recipients
7 are privy to the contents of their nonpublic communications. In reality, Facebook never intended
8 to provide this level of confidentiality. Instead, Facebook mines any and all transmissions across
9 its network, including those it labels “private,” in order to gather any and all morsels of
10 information it can about its users.

11 10. Plaintiffs Matthew Campbell and Michael Hurley are Facebook users who, during
12 the relevant Class Period, utilized Facebook’s private messaging function, each relying on
13 representations that these private and personal communications would be viewed only by the
14 sender and the recipient. Instead, where Plaintiffs sent private messages containing URLs,
15 Facebook scanned Plaintiffs’ messages and searched the website identified in the URL for
16 purposes including but not limited to data mining and user profiling.

17 11. While Facebook hides the extent of this intrusive behavior from its users, it is
18 candid about these activities in its technical guidance for web developers. Web developers are
19 computer programmers who specialize in the development of internet applications, or distributed
20 network applications that are run from a web server⁹ to a web browser,¹⁰ over HTTP.¹¹ Web

21 ⁷ *Reach the right people*, Facebook, [https://www.facebook.com/business/a/online-sales/target-](https://www.facebook.com/business/a/online-sales/target-your-ads)
22 [your-ads](https://www.facebook.com/business/a/online-sales/target-your-ads).

23 ⁸ *How to target Facebook ads*, Facebook, [https://www.facebook.com/business/a/online-sales/ad-](https://www.facebook.com/business/a/online-sales/ad-targeting-details)
24 [targeting-details](https://www.facebook.com/business/a/online-sales/ad-targeting-details).

25 ⁹ A web server can refer to either the hardware (the computer) or the software (the computer
26 application) that helps deliver web content that can be accessed through the Internet.

27 ¹⁰ A web browser is a software application for retrieving, presenting and traversing information
28 resources on the Internet.

¹¹ HTTP or “Hypertext Transfer Protocol” is a set of standards that allows users of the World
Wide Web to exchange information found on web pages. When an internet user enters “http://” in
front of a web address, this tells the web browser to communicate over HTTP. An HTTP request
is a request sent by a “client” to a “server” via the internet, asking for information contained on
the server. The most common example of this is when a web browser (e.g., Internet Explorer)
sends a request to a server to call up the information associated with a web page’s URL. For

1 developers are website administrators to whom Facebook offers or allows access to data created
 2 by its users' web traffic. Some of these web developers work at Facebook, while others work for
 3 companies that do business with Facebook, and still others are freelancers or contractors.

4 12. This class action is brought on behalf of all natural person Facebook users located
 5 within the United States who have sent or received private Facebook messages that included a
 6 URL in the content of the Facebook message. Upon information and belief, Facebook read these
 7 private Facebook messages.

8 13. Such actions, described in detail below, are intentional interceptions of electronic
 9 communications, committed in violation of the Electronic Communications Privacy Act,
 10 18 U.S.C. §§ 2510 *et seq.* ("ECPA"), California's Invasion of Privacy Act, Cal. Penal Code
 11 §§ 630 *et seq.* ("CIPA"), and the California Unfair Competition Law ("UCL").

12 14. Under ECPA, the CIPA, and the UCL, Plaintiffs seek, individually and on behalf
 13 of the Class, injunctive and declaratory relief, restitution, statutory damages, an award of
 14 reasonable attorney's fees and other litigation costs reasonably incurred, and any and all
 15 additional relief deemed appropriate by this Court.

16 **II. THE PARTIES**

17 15. Plaintiff Matthew Campbell a resident of Pulaski County, Arkansas. He
 18 established a Facebook account in or around January 2009, which he has maintained consistently
 19 to the present day. He has used Facebook's private messaging function throughout the relevant
 20 Class Period for, *inter alia*, purposes of conveying messages whose content includes URL links.

21 16. Plaintiff Michael Hurley is a resident of North Plains, Oregon. He established a
 22 Facebook account in or around October 2008, which he has maintained consistently to the present
 23 day. He has used Facebook's private messaging function throughout the relevant class period for,
 24 *inter alia*, purposes of conveying messages whose content contains URL links.

25
 26
 27 instance, where one enters the URL "www.nytimes.com" into the address bar of a web browser
 28 (the client) and hits the "Enter" button on the keyboard, the web browser will send a request to
 the *New York Times*' server for information associated with the front page of the *Times*' website.
 The server responds to the request by sending this information to the client, which then displays
 the webpage.

17. Defendant Facebook, Inc. is an American corporation, headquartered in Menlo Park, California, and incorporated under the laws of the State of Delaware. Facebook owns and operates an online social networking website that allows its users to communicate with each other through the sharing of text, photograph, and video.

III. JURISDICTION, VENUE, AND CHOICE OF LAW

18. Pursuant to 28 U.S.C. § 1331, this Court has original subject matter jurisdiction over the claims of Plaintiffs and the Class that arise under the Electronic Communications Privacy Act of 1986 (“ECPA”), 18 U.S.C. §§ 2510 *et seq.*

19. Further, this Court has subject matter jurisdiction over this putative nationwide class action pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005 (“CAFA”), because the matter in controversy exceeds \$5,000,000.00, exclusive of interest and costs, and is a class action in which some members of the Class are citizens of states different than Defendant. *See* 28 U.S.C. § 1332(d)(2)(A). Therefore, both elements of diversity jurisdiction under CAFA are present, and this Court has jurisdiction.

20. This Court has personal jurisdiction over Facebook because Facebook owns and operates a business that is headquartered in California, and because it conducts substantial business throughout California.

21. Venue properly lies in this district pursuant to 28 U.S.C. § 1391(b)(1), as Facebook is headquartered in this district.

22. Venue is also proper in this district pursuant to Facebook’s Statement of Rights and Responsibilities, which governs the agreement between Plaintiffs and Facebook and which states in pertinent part that Plaintiffs “will resolve any claim, cause of action or dispute (claim) . . . relating to . . . Facebook exclusively in a state or federal court located in Santa Clara County.”

23. California law governs the substantive legal issues in the instant matter, as Facebook’s Statement of Rights and Responsibilities further states in pertinent part that “the laws of the State of California will govern . . . any claim that might arise between you and us.”

1 **IV. FACTUAL BACKGROUND**

2 **A. Data Aggregation**

3 24. Many websites capitalize on the personal information they can collect from users.
4 Some sell the data directly; some use the data to build valuable profiles of users for sale or their
5 own use.

6 25. Data aggregation and sale are highly lucrative, both in the United States and
7 abroad. In the United States alone, data-driven marketing was reportedly worth \$156 billion in
8 2012,¹² whereas a recent Boston Consulting Group Report puts the numbers in Europe even
9 higher: it estimates a total “digital identity value” of Europeans in 2011 as €315 billion, a number
10 expected to reach €1 trillion by 2020.¹³

11 26. Even though many websites remove personally identifiable information from data
12 when they are initially sold, data aggregators are employing ever more sophisticated cross-
13 referencing and predictive analytics techniques to make more sources of data personally
14 identifiable.¹⁴

15 27. Widespread dissemination of even de-identified data is already causing problems
16 for internet users. Kate Crawford, a visiting professor at the MIT Center for Civic Media and a
17 principal researcher at Microsoft Research, and Jason Shultz, of the New York University School
18 of Law, explain the privacy risks arising from new methods of data aggregation and analysis:

19 Even very vague signals online, such as liking things on Facebook,
20 can generate a detailed picture. As one University of Cambridge
21 study found, ‘highly sensitive personal attributes,’ such as sexual
22 orientation, ethnicity, religious and political views, personality
23 traits, intelligence, use of addictive substances, parental separation,
24 age and gender were predictable with high degrees of success just
25 from what people liked online. Thus, racial discrimination could be
26 applied to prevent some candidates from seeing loans that might be

24 ¹²US Data Marketing ‘Worth \$156 bn,’ Warc (fka World Advertising Research Center) (Oct. 16, 2013),

25 http://www.warc.com/Content/News/N32077_US_data_marketing_worth_24156bn_content?CID=N32077&ID=6bba593a-da7f-433f-9030-c2c91452cc4b&q=direct+response+advertising&qr=

26 ¹³ The Value of Our Digital Identity, The Boston Consulting Group (Nov. 2012),

27 <http://www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf>.

28 ¹⁴ Kate Crawford and Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, New York University School of Law Public Law & Legal Theory Research Paper Series, Working Paper No. 13-64 at 8 (Oct. 2013), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2325784.

1 advantageous to them, and housing renters and sellers could
 2 potentially use big data to discriminate based on gender, all while
 3 circumventing the fair housing laws.¹⁵

4 28. Information that people never intended to make public can be used against them in
 5 other ways, such as to deny healthcare coverage. According to Crawford and Schulz:

6 [D]ata about our online behavior generally – such as buying an e-
 7 book about breast cancer survival or liking a disease foundation’s
 8 Facebook page – can also reveal information about our health . . .
 9 When these data sets are cross-referenced with traditional health
 10 information, as big data is designed to do, it is possible to generate
 11 a detailed picture about a person’s health, including information a
 12 person may never have disclosed to a health provider. The
 13 combination of data sets and use of predictive analytics can
 14 dramatically increase the amount of data that can be considered
 15 private.¹⁶

16 29. In another example of the uses to which data aggregators are putting predictive
 17 analytics, a recent New York Times blog post reported that one man saw his American Express
 18 credit card limit reduced because, according to American Express, “Other customers who have
 19 used their card at establishments where you recently shopped have a poor repayment history with
 20 American Express.”¹⁷

21 30. Even if a company only stores user information, and does not immediately use the
 22 data it gleans from users’ private messages to target advertisements or for any purpose directly
 23 associated with the individual, it may sell that information at its discretion, and it can be resold by
 24 any company that buys it. Companies that acquire user data can retain that information
 25 indefinitely and use it for any purpose not prohibited by law or contract.

26 31. This puts people at risk of crime, discrimination, or embarrassment, and they are
 27 powerless to stop it because once a company like Facebook obtains their data, users have no
 28 control over subsequent analysis, sale, or other use of the data.

29 32. Widespread dissemination of information about individuals empowers the
 30 government against citizens to a degree well beyond the contemplation of the Fourth

31 ¹⁵ *Id.*

32 ¹⁶ *Id.* at 6.

33 ¹⁷ Lily Altavena, *What Story Does Your Personal Data Tell?*, N.Y. Times, The Learning Network
 34 (Feb. 17, 2013), <http://learning.blogs.nytimes.com/2012/02/07/what-story-does-your-personal-data-tell/>.

Amendment. Facebook declares that it only provides the stored contents of any account to the government with a warrant,¹⁸ yet it has been reported that the companies that purchase such information can hand it over to government agencies with no probable cause and with no warrant.¹⁹

33. Foreign regimes may also gain access to users' private data after it has been aggregated by companies like Facebook.²⁰

34. Furthermore, if companies like Facebook do not have to adhere to terms of their own policies and representations regarding what data they collect, there is no basis for consumer trust. Ultimately, the duplicity alleged herein by entities like Facebook will likely cause consumers to assume that all communications they make are recorded and disseminated, significantly chilling free speech.

35. In response to the threats posed by internet privacy invasions, the Department of Commerce has recently recommended basic principles for internet regulation that align with the goals underlying the CIPA and the ECPA. First articulated by the Department of Health and Human Services more than 30 years ago, they are known as the Fair Information Practice Principles ("FIPPs"). The FIPPs stand for eight relatively straightforward ideas:

- Transparency: Individuals should have clear notice about the data collection practices involving them.
- Individual Participation: Individuals should have the right to consent to the use of their information.
- Purpose Specification: Data collectors should describe why they need particular information.
- Data Minimization: Information should only be collected if it is needed.

¹⁸ *Information for Law Enforcement Authorities*, Facebook, <https://www.facebook.com/safety/groups/law/guidelines/>.

¹⁹ American Civil Liberties Union, *Focus on Data Aggregation*, at 2 (June 2010) ("The federal government is also a customer of private data companies. It's cheaper to buy information that's already been assimilated; it also avoids warrants or court oversight.")

²⁰ Repressive regimes like Iran have demonstrated an interest in the online activities of U.S. citizens. For example, dozens of American Facebook users who posted political messages critical of Iran have reported that Iranian authorities subsequently questioned and detained their relatives. Electronic Privacy Information Center, *Frequently Asked Questions Regarding EPIC's Facebook Complaint*, <http://epic.org/privacy/socialnet/fbfaq.html>.

- Use Limitation: Information collected for one purpose should not be used for another.
- Data Quality and Integrity: Information should be accurate.
- Security: Information should be kept secure.
- Accountability and Auditing: Data collectors should know who has accessed information and how it is used.

B. Facebook

36. With 1.1 billion users accessing this service on a monthly basis – approximately 51% of all internet users – Facebook is the world’s largest social media company.

37. The popularity of Facebook hinges upon the ability of its users to communicate with one another. As the Company stated in a Securities and Exchange Commission filing in anticipation of its May 2013 initial public offering or “IPO,” “[p]eople use Facebook to stay connected with their friends and family, to discover what is going on in the world around them, and to share and express what matters to them to the people they care about. . . . We believe that we are at the forefront of enabling faster, easier, and richer communication between people and that Facebook has become an integral part of many of our users’ daily lives.”²¹

38. Communications among Facebook users span a continuum, from the publicly viewable to the entirely private. In the Facebook tutorial “Get Started on Facebook,” guidance is offered on how to share or send information via the service, either publicly or privately:

▪ How to Post & Share

▪ Sharing Status Updates and Other Stories

How do I share a status or other content on Facebook?

Depending on whom you’d like to share with, there are different ways to share content on Facebook:

- **Sharing with a broad audience:** Use the share menu that’s located at the top of your homepage and timeline to let others know what’s on your mind. You can update your status and share photos, videos, links and other application content. Things you share will appear as posts on your timeline, and can appear in your News Feed. To control whether or not

²¹ Form S-1 Registration Statement for Facebook, Inc., as filed with the Securities and Exchange Commission, “Prospectus Summary,” at 1 (Feb. 1, 2012), <http://www.sec.gov/Archives/edgar/data/1326801/000119312512034517/d287954ds1.htm>.

specific people have the option to view your stories, you can change the privacy settings for each piece of content you post.

- **Sharing with a small group of friends:** Use the Groups feature to share content with a select group of people, like family members, your soccer team or your book club.
- **Sharing with an individual:** You can use the share menu at the top of a friend's timeline to write or share something on his or her timeline. Friends of your friend will also be able to view your post. ***If you'd like to share something privately, you can always send someone a private message.***²²

39. Thus, Facebook states that its private messaging function is meant to be precisely that: a “private” mechanism for communication between individuals using the Company’s services. Further, Facebook telegraphs through the use of the words “privately” and “private” that when a user sends a private message to another party, only the user and the intended recipient will be privy to the contents of that communication.

1. Facebook’s Private Messaging Function

40. On November 15, 2010, Facebook announced a new, integrated email and messaging service for its users. Combining the functionality of email, chat, SMS,²³ and in-service messaging into a single platform, Facebook’s private messaging service enables Facebook users to communicate directly with specifically chosen individuals, in a single conversation, across devices and through a variety of popular media.²⁴ Because the messaging service can also serve as an email address, account holders can also use Facebook as a means of sending messages to, and receiving messages from, sources outside the Company’s social media network.

41. Facebook took special pains to tout the privacy features of its new private messaging service. In its rollout announcement, it said “[y]ou can also change your account settings to be even more limited and bounce any emails that aren’t exclusively from friends. This kind of message control is pretty unprecedented and people have been wanting to do this with email (and phone calls) for a long time. *‘Messages’ reverses the approach to preventing*

²² *Help Center: Get Started on Facebook: How to Post & Share* (italic and bold emphasis added).

²³ “SMS” is an acronym for “short message service,” commonly known as “text messaging.”

²⁴ *See the Messages that Matter*

1 *unwanted contact. Instead of having to worry about your email address getting out, you're now*
 2 *in control of who can actually reach you.”*²⁵

3 42. Thus, in Facebook's inaugural representations of its private messaging service, it
 4 stressed “unprecedented” amounts of (1) user control and (2) user privacy inherent in its product.

5 43. Where Facebook discusses its private messaging service on its website, it does so
 6 in terms that expressly contemplate a *private* communication, taking place only between the
 7 sender and the intended recipient or recipients (*e.g.*, “If you'd like to share something *privately*,
 8 you can always send someone a *private* message”²⁶ and “unprecedented” levels of “message
 9 control”²⁷). Additionally, Facebook's website contains a “Help Center” which assists account
 10 holders in utilizing basic functions of the service. In the Help Center, under the heading “How do
 11 I send a message” the step-by-step instruction begins with the prompt “To send a *private*
 12 message.”²⁸ Under the heading “Who can see my message,” Facebook states “You and the
 13 people you're messaging with can view the contents and history of your conversation.”²⁹

14 44. All of these representations reflect the promise that only the sender and the
 15 recipient or recipients will be privy to the private message's content, to the exclusion of any other
 16 party, including Facebook.

17 2. Third-Party Security Researchers Demonstrate that Facebook is 18 Intercepting and Scanning the Content of “Private” Messages

19 45. Facebook's representations of privacy have been discredited by security
 20 researchers over the past year. Facebook has been caught surreptitiously intercepting and
 21 scanning the contents of its users' private messages for a variety of purposes, none of which
 22 Facebook discloses in either its Terms of Use or its Privacy Policy.

23
 24 ²⁵ *Id.* (emphasis added).

25 ²⁶ *Help Center: Get Started on Facebook: How to Post & Share* (emphasis added).

26 ²⁷ *See the Messages that Matter*

27 ²⁸ *Help Center: Messaging: Messages: Sending a Message: How Do I Send a Message?*,
 Facebook, <https://www.facebook.com/help/326534794098501/>, (emphasis added).

28 ²⁹ *Help Center: Messaging: Messages: Settings & Security: Who Can See My Messages?*,
 Facebook,
<https://www.facebook.com/help/212388195458335?sr=16&sid=0ntT7VdfDjw7Y5KSV>.

1 46. On August 27, 2013, a Swiss security firm announced that it had conducted a
 2 simple experiment to test how scrupulously the fifty largest social networks, web services, and
 3 free email systems (“Web Services”) respected user privacy.³⁰ The firm, High-Tech Bridge
 4 (“HTB”), used a dedicated web server and generated a secret URL for each of the Web Services.
 5 HTB then used the private messaging function of each of the Web Services, embedding a unique
 6 URL in each message.

7 47. HTB then monitored its dedicated web server’s logs for all incoming HTTP
 8 requests, in order to see whether any of the Web Services would “click” on the test URLs that had
 9 been transmitted via private message.

10 48. Facebook was one of the Web Services that was caught scanning URLs despite
 11 such activity remaining undisclosed to the user.

12 49. Concerning Facebook’s scanning of the contents of privately sent messages,
 13 HTB’s Chief Research Officer stated, “there is no way to keep the URL and its content
 14 confidential . . . while transferring the URL via social networks.”³¹

15 50. Facebook performs this task to aggregate data on its users for purposes of
 16 advertising, marketing and user profiling; specifically, at least in part, in the form of generating
 17 “Likes” for web pages, generated via Facebook’s social plugins embedded on websites, thereby
 18 monitoring users’ web browsing patterns.

19 3. Facebook’s Social Plugins

20 51. In addition to having users interact on its own website, Facebook also provides
 21 code for third-party websites to embed, so-called “social plugins.” Facebook explains the social
 22 plugin as follows,

23 Alright, so this is how it works. Let’s say you are logged in to
 24 Facebook, but you check out a popular new site. It’s kind of a
 25 bummer, because before you would have to choose between the
 26 social experience of Facebook or the specialized information of a
 content site. Ok, well now, if the website has a social plug-in, you
 can take your Facebook friends with you and get both. Instead of
 having to comb through page after page of article after article to

27 ³⁰ High-tech Bridge, *Social Networks: Can Robots Violate User Privacy?* (Aug. 27, 2013),
 28 https://www.htbridge.com/news/social_networks_can_robots_violate_user_privacy.html.

³¹ *Id.*

find something that catches your eye, now you can see what your friends have already enjoyed on a site. And with one click, you can share an article or a video review with your friends.³²

52. The effect of embedding social plugins into third-party websites is that it enables Facebook to extend its data gathering practices, keeping tabs on its users' behavior even after they log out of Facebook. One of the principal social plugins is the "Like" button commonly found on internet websites.³³ A video tutorial on Facebook's website states:

When someone clicks "Like," they're highlighting the things that are valuable to them and sharing that with their friends. And when all of this goes to your News Feed, it's like you have a real time, super-customized window to the most valuable things on the Internet. But we understand that many of the things people care about live outside of Facebook, so we wanted to create a way to bring your friends with you to other websites. So we created social plugins. Social plugins extend the things you love about Facebook to your favorite websites.³⁴

53. In practice, Facebook social plugins serve as an extension of Facebook on the internet at large. In addition to Facebook's "Like" button at the top of a news article, Facebook's social plugins can take the form of a sidebar feed noting any friends who have read or recommended the article, or a clickable Facebook icon, as circled below.

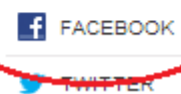
NEWS ANALYSIS

The Information-Gathering Paradox

By SOMINI SENGUPTA

Published: October 26, 2013

SAN FRANCISCO — CONSUMER trust is a vital currency for every big Internet company, which helps to explain why the giants of



54. If users are concerned that their extra-Facebook web traffic is being broadcast across the world's largest social network, the Company offers this assurance:

When you start to see websites that are customized for you all over the Internet, you might wonder if everyone else can see it. But it's not like that. Although you can see customized information on other sites, all the information lives on Facebook, and Facebook

³² *Understanding Social Plugins*, Facebook tutorial video at 0:40 – 1:09 (posted June 7, 2010), <https://www.facebook.com/video/video.php?v=10150210521510484>.

³³ *Id.* (listing the "Like" button as one of "the main social plugins.").

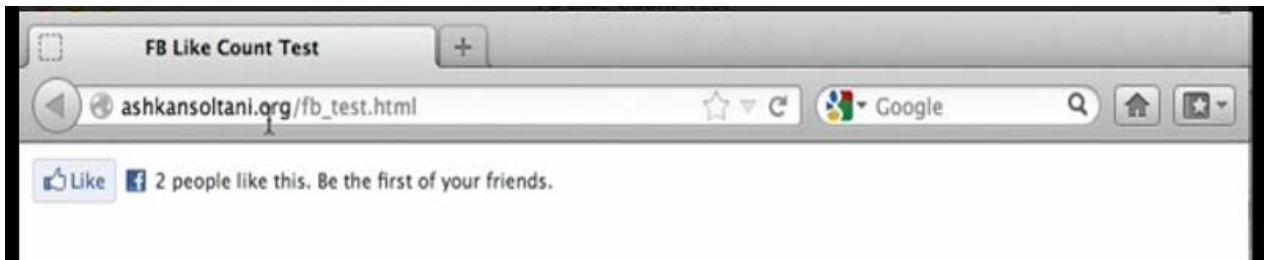
³⁴ *Id.* at 0:15 – 0:39

³⁵ Somini Sengupta, *The Information Gathering Paradox*, N.Y. Times, Oct. 26, 2013.

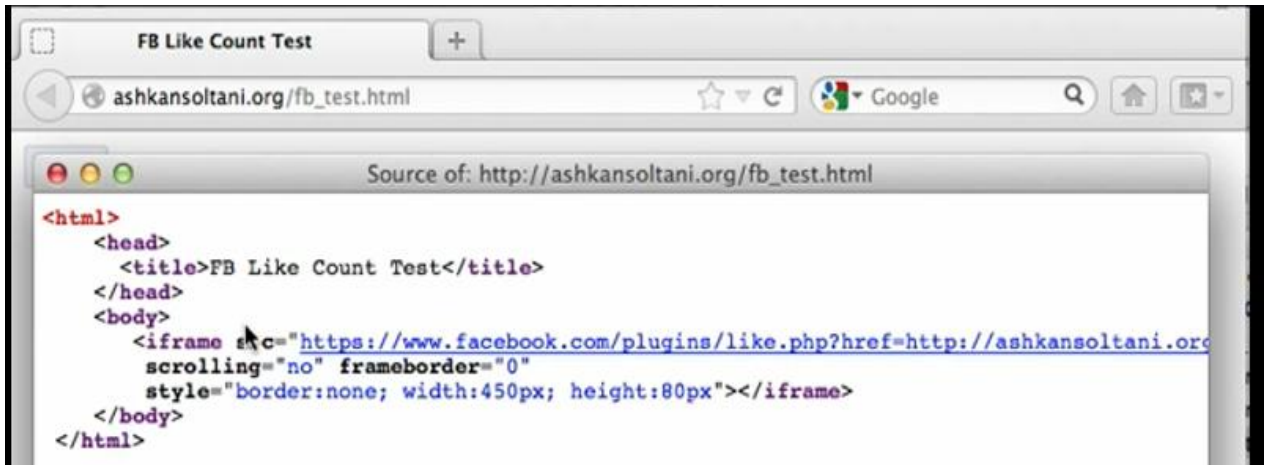
doesn't share your information with anyone through social plugins. And each person has full control of what they want to share. You're only sharing the information you want to, and you're only sharing it with the people you want to share it with.³⁶

55. In October 2012, a security researcher published findings in the *Wall Street Journal* showing that Facebook scans users' private messages for URLs.³⁷ When a private message contains a link to a third-party website, and that website has a "Like" social plugin, Facebook registers up to two "Likes" for that web page via the social media plugin.³⁸

56. In this first screenshot, the website set up by the security researcher, Ashkan Soltani, "ashkansoltani.org/fb_test.html," has two (2) likes registered to it.



Soltani also provided the html code for the website:

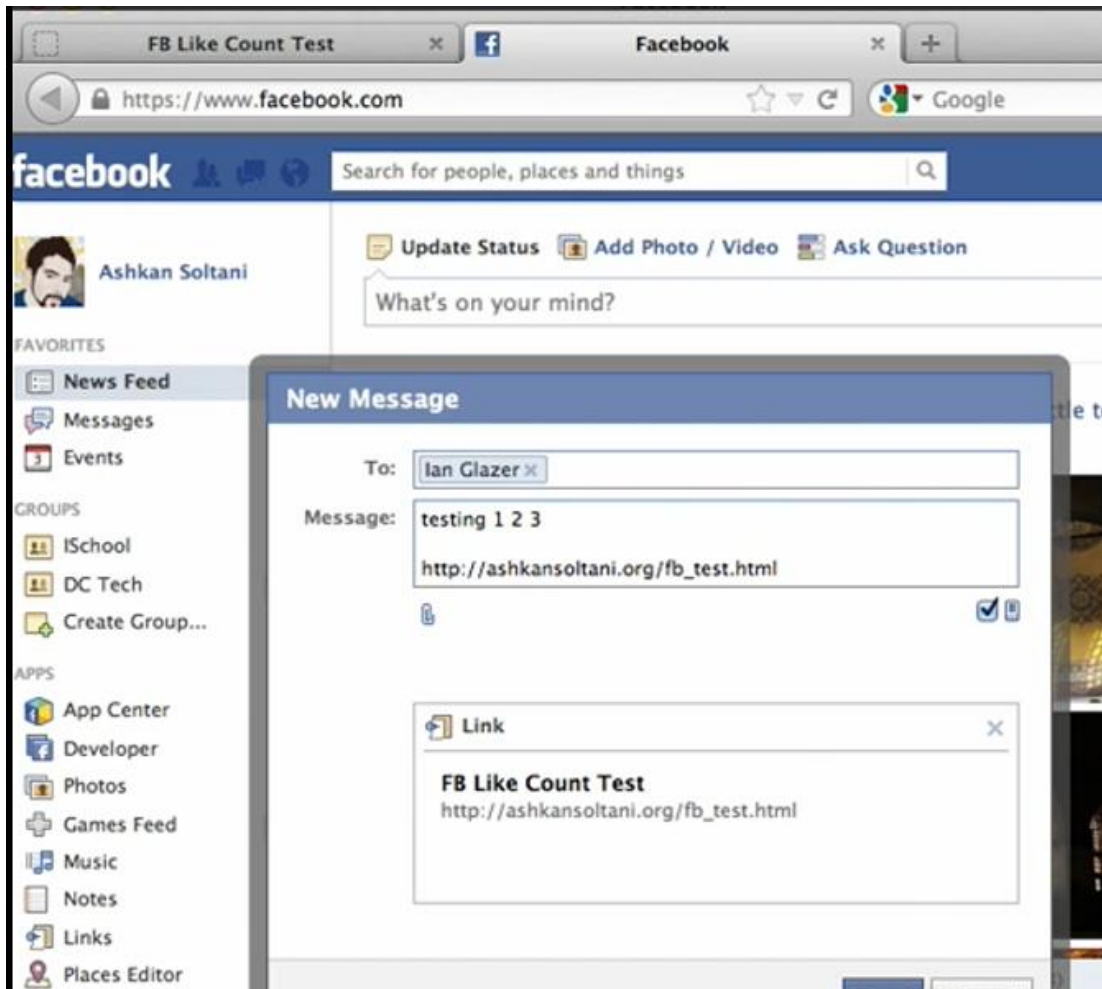


Soltani then logged into Facebook and sent a message that contained the URL and the text "testing 1 2 3."

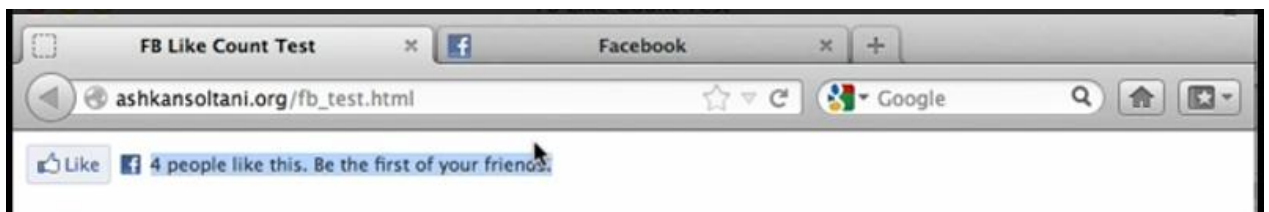
³⁶ *Understanding Social Plugins*, at 1:14 – 1:37 (emphasis added).

³⁷ Jennifer Valentino-DeVries and Ashkan Soltani, *How Private Are Your Private Facebook Messages?*, Wall St. J., Oct. 3, 2012.

³⁸ *Id.*



Finally, Soltani navigated back to his test website to see if the number of “Likes” registered to it increased, which they did.³⁹



57. The article notes that this practice is described in Facebook’s guidance for developers – administrators of the third-party websites whom Facebook seeks to entice to use social plugins. The developer guidance states that “the number of inbox messages containing” a

³⁹Indeed, as a result of a technical glitch at the time, Facebook added two “Likes” per URL instead of one. A video showing Soltani complete this test in real-time can be found as part of the Digital Trends article reporting on it. See Molly McHugh, *Facebook Scans Private Messages for Brand Page Mentions, Admits a Bug Is Boosting Likes*, Digital Trends (Oct. 4, 2012), <http://www.digitaltrends.com/social-media/facebook-scans-private-messages/>.

link to a page will count as ‘Likes.’”⁴⁰ However, this practice – scanning private messages and doling out “Likes” to websites if a hyperlink is contained therein – is *not* disclosed anywhere in Facebook’s Privacy Policy.

58. Beyond scanning messages for social plugin purposes, Facebook also has conceded that it uses a combination of software and human screening to comb through private messages and search for criminal activity.⁴¹ Upon information and belief, this practice extends beyond the scanning of URLs and involves a combination of keyword searches, user profiling, and other, “extensive but little discussed technology,”⁴² all of which enables Facebook to gather additional private information about its users.

59. As discussed in paragraph 63, the “Like” function is crucial in gathering data points for the profiles Facebook keeps on its users for profit, including for purposes of delivering targeted advertising.

60. The practice, purpose, and effect of scanning users’ private messages, as described herein, are not disclosed by Facebook to its users, and these scans are undertaken without users’ consent.

61. The practice, purpose, and effect of scanning users’ private messages, as described herein, are not necessary for the rendition of Facebook’s private messaging service, the protection of Facebook’s rights or property, or the security of Facebook users. These scans are not undertaken in the ordinary course of business of an electronic communication service, as described in 28 U.S.C. § 2510(15).

4. **Facebook’s Incentive: Mining User Data**

62. As information is shared by its more than one billion unique users, Facebook is provided with sophisticated, exceedingly detailed data profiles. These vast databases of individual user information and behavior, coupled with proprietary analytics algorithms, enable

⁴⁰ *Id.*, citing Facebook.com, *Facebook Developers: Social Plugins: Like Button*, <https://developers.facebook.com/docs/plugins/like-button/>.

⁴¹ Joseph Menn, *Social Networks Scan For Sexual Predators, With Uneven Results*, Reuters (July 12, 2012), <http://www.reuters.com/article/2012/07/12/us-usa-internet-predators-idUSBRE86B05G20120712>.

⁴² *Id.*

Facebook to surgically place ads throughout users' accounts based upon the extensive profiles assembled on each and every user. As the Company explains:

When an advertiser creates an ad, they are given the opportunity to choose their audience by location, demographics, likes, keywords, and any other information we receive or can tell about you and other users. For example, an advertiser can choose to target 18 to 35 year-old women who live in the United States and like basketball. An advertiser could also choose to target certain topics or keywords, like "music" or even people who like a particular song or artist. If you indicate that you are interested in topics, such as by liking a Page, including topics such as products, brands, religion, health status, or political views, you may see ads related to those topics as well.

Sometimes we allow advertisers to target a category of user, like a "moviegoer" or a "sci-fi fan." We do this by bundling characteristics that we believe are related to the category. For example, if a person "likes" the "Star Trek" Page and mentions "Star Wars" when they check into a movie theater, we may conclude that this person is likely to be a sci-fi fan. Advertisers of sci-fi movies, for example, could ask us to target "sci-fi fans" and we would target that group, which may include you. Or if you "like" Pages that are car-related and mention a particular car brand in a post, we might put you in the "potential car buyer" category and let a car brand target to that group, which would include you.⁴³

63. As the above statement by the Company makes clear, "Likes" are essential to Facebook in its creation of data profiles for each of its users. These data profiles in turn enable Facebook to deliver ads with industry-leading accuracy. According to a third-party study, broadly targeted campaigns on Facebook (*e.g.*, adults between the ages of 25 and 49) reach the desired audience with 95% accuracy, compared with an industry average of 72%; for more narrowly targeted campaigns (*e.g.*, females between the ages of 25 and 34), Facebook reaches the desired audience with 90% accuracy, compared to an industry average of just 35%.⁴⁴

64. In 2009, 2010, and 2011, targeted advertising accounted for 98%, 95%, and 85%, respectively, of the Company's revenue.⁴⁵

⁴³ *Data Use Policy, IV. How Advertising and Sponsored Stories Work*, Facebook (updated Dec. 11, 2012), <http://www.scribd.com/doc/191118234/Facebook-2>.

⁴⁴ Form S-1 Registration Statement for Facebook, Inc., *How We Create Value for Advertisers and Marketers*, 76.

⁴⁵ *Id.*, *Risks Related to Our Business and Industry*, 12.

65. However, as discussed throughout this Complaint, Facebook's desire to harness the myriad data points of its users has led to overreach and intrusion on the part of the Company as it mines its account holders' private communications for monetary gain.

C. Facebook Employs Devices and/or Technology to Scan, Extract, Acquire, and Use the Contents of Its Users' Messages.

1. Web Crawlers and Social Plugins

66. Upon information and belief, Facebook uses a software application called a "web crawler" to scan any URL contained in a user's private message.

67. These web crawlers perform the automated task of scanning the URL by sending HTTP requests to the server associated with the URL and then seeking various items of information about the web page to which the URL is linked.

68. As discussed in paragraphs 51-54, Facebook has developed items of code called "social plugins," which can be embedded in third-party websites and, when clicked on by visitors, interact with Facebook.

69. Such social plugins include, among others, the "Like" button.⁴⁶

70. Upon information and belief, one of the items of information Facebook's web crawlers seek is whether or not the web page associated with the URL contains a "Like" button.

71. Upon information and belief, where a web page *does* contain a "Like button, the web crawlers transmit this information back to Facebook.

72. Upon information and belief, Facebook then uses these data to register the URL sent via private message as a "Like" for the web page.

73. Upon information and belief, Facebook further provides these data to the web page at issue, in the form of analytical analysis of web traffic to that site by Facebook users.

74. Upon information and belief, Facebook further uses these data to build and refine user profiles.

75. Upon information and belief, Facebook's interception occurs in transit, in transmission, and/or in transfer of users' private messages.

⁴⁶ *Product Docs: Social Plugins*, Facebook, <https://developers.facebook.com/docs/plugins/>.

2. **Facebook's Message-Scanning Devices and/or Technology Constitute Conduct Outside the Scope of the Company's Ordinary Course of Business.**

76. None of the practices complained of throughout this complaint are necessary for or incidental to the ability to send or receive private messages – an electronic communication service – across Facebook's online social network.

77. Facebook has the technical capacity to offer its private message service without intercepting, scanning, and using the content of Plaintiffs' and Class Members' private messages.

78. Facebook's acquisition and use of content from Plaintiffs' and Class Members' electronic communications, as described in this Complaint, is not necessary for or incidental to the protection of the rights or property of the Company, as provider of the service. Indeed, such activities, as described herein, are outside the ordinary course of business of electronic communication service providers.

D. **Facebook Fails to Disclose That Its Private Message Processes Read, Acquire, and Use Private Message Content, in Violation of Its Express Agreements With Facebook Users.**

1. **No user consents to Facebook's unlawful conduct because Facebook's Statement of Rights and Responsibilities and Privacy Policy are silent on the private-message-scanning processes.**

79. In order to establish a Facebook account, a user must agree to the Company's Statement of Rights and Responsibilities and its Privacy Policy. Specifically, on Facebook's main page, it states, "By clicking Sign Up, you agree to our Terms and that you have read our Data Use Policy, including our Cookie Use."⁴⁷ Within this sentence, the word "Terms" contains a hyperlink, leading to Facebook's "Statement of Rights and Responsibilities,"⁴⁸ similarly, the words "Data Use Policy" contain a hyperlink, leading to Facebook's "Data Use Policy."⁴⁹

2. **Facebook's Statement of Rights and Responsibilities**

80. The Statement of Rights and Responsibilities informs users that

This Statement of Rights and Responsibilities ("Statement," "Terms," or "SRR") derives from the Facebook Principles, *and is our terms of service that governs our relationship with users* and

⁴⁷ Facebook, <https://www.facebook.com>.

⁴⁸ *Statement of Rights and Responsibilities*, Facebook, <https://www.facebook.com/legal/terms>.

⁴⁹ *Data Use Policy*, Facebook, <https://www.facebook.com/about/privacy>.

others who interact with Facebook. By using or accessing Facebook, you agree to this Statement, as updated from time to time in accordance with Section 14 below. Additionally, you will find resources at the end of this document that help you understand how Facebook works.

(emphasis added).

81. The very first enumerated section of the Statement of Rights and Responsibilities is titled “Privacy.” It consists of three sentences:

Your privacy is very important to us. We designed our Data Use Policy⁵⁰ to make important disclosures about how you can use Facebook to share with others and how we collect and can use your content and information. We encourage you to read the Data Use Policy, and to use it to help you make informed decisions.

82. The above language incorporates Facebook’s Data Use Policy by reference, and designates this document as governing the Company’s privacy policy with its users.

3. Facebook’s Data Use Policy

83. The term “message” is found in Facebook’s Data Use Policy (“the Policy”) only nine times, and only once contemplates the Company receiving data related to users’ private messages. Specifically, under the heading “Information we receive and how it is used,” the Company states:

Other information we receive about you

We also receive other types of information about you:

- We receive data about you whenever you use or are running Facebook, such as when you look at another person’s timeline, send or receive a message, search for a friend or a Page, click on, view or otherwise interact with things, use a Facebook mobile app, or make purchases through Facebook.⁵¹

⁵⁰ As with the disclosure on the main page, “www.facebook.com,” the words “Data Use Policy” contain a hyperlink leading to <https://www.facebook.com/about/privacy/>.

⁵¹ Data Use Policy: Information we receive and how it is used, Facebook, https://www.facebook.com/full_data_use_policy. There have been minor revisions to this language during the class period, not one of which is material to the allegations contained herein. Prior to November 15, 2013, this language read: “We receive data about you whenever you interact with Facebook, such as when you look at another person’s timeline, send or receive a message, search for a friend or a Page, click on, view or otherwise interact with things, use a Facebook mobile app, or purchase Facebook Credits or make other purchases through Facebook.”

1 84. Under the section titled “How we use the information we receive,” the Policy
2 states:

3 We use the information we receive about you in connection with
4 the services and features we provide to you and other users like
5 your friends, our partners, the advertisers that purchase ads on the
6 site, and the developers that build the games, applications, and
7 websites you use. For example, in addition to helping people see
8 and find things that you do and share, we may use the information
9 we receive about you:

- 10 ▪ as part of our efforts to keep Facebook products, services and
- 11 integrations safe and secure;
- 12 ▪ to protect Facebook’s or others’ rights or property;
- 13 ▪ to provide you with location features and services, like telling
- 14 you and your friends when something is going on nearby;
- 15 ▪ to measure or understand the effectiveness of ads you and
- 16 others see, including to deliver relevant ads to you;
- 17 ▪ to make suggestions to you and other users on Facebook, such
- 18 as: suggesting that your friend use our contact importer because
- 19 you found friends using it, suggesting that another user add you
- 20 as a friend because the user imported the same email address as
- 21 you did, or suggesting that your friend tag you in a picture they
- 22 have uploaded with you in it; and
- 23 ▪ for internal operations, including troubleshooting, data analysis,
- 24 testing, research and service improvement.

25 ***

26 While you are allowing us to use the information we receive about
27 you, you always own all of your information. Your trust is
28 important to us, which is why we don’t share information we
receive about you with others unless we have:

- 29 ▪ received your permission;
- 30 ▪ given you notice, such as by telling you about it in this policy;
- 31 or
- 32 ▪ removed your name or any other personally identifying
- 33 information from it.

34 85. These disclosures do not disclose that *as a matter of course* Facebook scans,
35 mines, and manipulates the content of its users’ private messages, acting in a manner in direct
36 conflict with the assurances it provides to its users regarding the privacy and control they should
37 expect in using Facebook’s services. See ¶¶ 38-44, etc., *supra*.

1 86. In contrast to its disclosures to developers discussed in paragraph 57, *supra*,
2 Facebook's disclosures to users do not state that Facebook scans URLs transmitted via private
3 message across its social network.

4 87. In contrast to its disclosures to developers discussed in paragraph 57, *supra*,
5 Facebook's disclosures to users do not state that Facebook will register the fact that a URL is
6 communicated privately, via its private message function, as a "Like" for a particular web page.

7 88. In contrast to its disclosures to developers discussed in paragraph 57, *supra*,
8 Facebook's disclosures to users do not state that, when a user sends a URL as part of a private
9 message, this act will become part of Facebook's data profile of web traffic for the linked-to
10 website.

11 89. In contrast to its disclosures to developers discussed in paragraph 57, *supra*,
12 Facebook's disclosures to users do not state that, when a user sends a URL as part of a private
13 message, this act will become part of Facebook's data profile of the user.

14 90. Instead, Facebook misleads users into believing that they have a secure, private
15 mechanism for communication – Facebook's private messaging function – when, in fact,
16 Facebook intercepts and scans the content and treats portions of that content no differently than a
17 public "Like" or post, broadcast openly across the Internet. Further, the purpose for the invasive
18 scanning of these purportedly "private" messages is not meant for the benefit of users, but rather
19 is a mechanism for Facebook to surreptitiously gather data in an effort to improve its marketing
20 algorithms and increase its ability to profit from data about Facebook users.

21 **CLASS ALLEGATIONS**

22 91. Plaintiffs bring this nationwide class action, pursuant to Rule 23 of the Federal
23 Rules of Civil Procedure, individually and on behalf of all members of the following Class:

24 All natural person Facebook users located within the United States
25 who have sent or received private messages where such message
26 included URLs in the content, from within two years before the
filing of this action up through and including the date of the
judgment in this case.

27 92. Excluded from the Class are the following individuals and/or entities: Facebook
28 and its parents, subsidiaries, affiliates, officers and directors, current or former employees, and

any entity in which Facebook has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

93. Plaintiffs reserve the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

94. The Class is so numerous that joinder of all members is impracticable. Upon information and belief, there are more than 166 million Facebook account holders in the United States. The number of separate individuals who sent private messages via Facebook, where such message included URLs in the content, within two years before the filing of this action, is likely in the millions, and is identifiable and ascertainable based on Facebook's records.

95. There are questions of law or fact common to the Class. These questions include, but are not limited to, the following:

a. Whether Facebook intentionally intercepted, endeavored to intercept, or procured any other person to intercept or endeavor to intercept Plaintiffs' and Class Members' electronic communications sent via Facebook;

b. Whether Facebook intentionally used, or endeavored to use, the contents of Plaintiffs' and Class Members' electronic communications sent via Facebook, knowing or having reason to know that the information was obtained in violation of 18 U.S.C. § 2511(1)(d);

c. Whether Facebook acted intentionally in violating privacy rights;

d. Whether Facebook acquired any "contents" of Plaintiffs' and Class Members' private messages, within the meaning of 18 U.S.C. § 2510(8);

e. Whether Plaintiffs' and Class Members' private messages sent via Facebook were "electronic communications" within the meaning of 18 U.S.C. § 2510(12);

f. Whether Facebook used an "electronic, mechanical, or other device," within the meaning of 18 U.S.C. § 2510(5);

g. The amount of statutory damages that should be levied against Facebook;

1 h. Whether injunctive and/or declaratory relief against Facebook should be
2 awarded;

3 i. Whether Facebook's conduct was likely to deceive its users;

4 j. Whether Facebook's conduct was unlawful; and

5 k. Whether Plaintiffs and Class Members are entitled to restitution.

6 96. Plaintiffs' claims are typical of the claims of the Class in that Plaintiffs and the
7 Class sent and/or received private messages via Facebook, where such messages contained URLs
8 in the content. In the process, Facebook intercepted, scanned, and acquired the private messages'
9 content, sending HTTP requests to the servers housing the web pages referred to in Plaintiffs' and
10 Class Members' private messages. Facebook further used or endeavored to use the contents of
11 Plaintiffs' and Class Members' private messages, where the Company found URLs to webpages
12 containing social plugins, manipulating such social plugins to generate "Likes" for web pages and
13 to assemble profiles of users' web traffic and personal preferences. Plaintiffs and Class Members
14 did not consent to the interception and uses of their private message content, which comprise the
15 basis for this suit. Plaintiffs and Class Members are entitled to declaratory relief, statutory
16 damages, restitution, and injunctive relief as a result of the conduct complained of herein.
17 Moreover, upon information and belief, the conduct complained of herein is systemic. Thus, the
18 representative Plaintiffs, like all other Class Members, face substantial risk of the same injury in
19 the future. The factual basis of Facebook's conduct is common to all Class Members, and
20 represents a common thread of conduct resulting in injury to all members of the Class. Plaintiffs
21 have suffered the harm alleged and have no interests antagonistic to any other Class Member.

22 97. Plaintiffs will fairly and adequately protect the interests of the Class. Plaintiffs'
23 interests do not conflict with the interests of the Class Members. Furthermore, Plaintiffs have
24 retained competent counsel experienced in class action litigation. Plaintiffs' counsel will fairly
25 and adequately protect and represent the interests of the Class. Fed. R. Civ. P. 23(a)(4) and 23(g)
26 are satisfied.

27

28

1 105. Facebook's actions are and have been intentional as evidenced by, *inter alia*, its
2 disclosures to developers and the design and implementation of its private messaging service,
3 web crawlers, and social plugins.

4 106. Facebook's actions complained of herein are not necessary practices for providers
5 of electronic communications, nor are they incidental to the act of facilitating private messages
6 across Facebook's social network.

7 107. Pursuant to 18 U.S.C. § 2511(1)(a), Facebook intentionally intercepted, intercepts,
8 or endeavored or endeavors to intercept the electronic communications of Plaintiffs and Class
9 Members.

10 108. Through Facebook's scanning of users' private messages, the Company acquired
11 and continues to acquire the substance, purport, and meaning of private messages transmitted to
12 and from Plaintiffs and Class Members.

13 109. The private messages transmitted to and from Plaintiffs and Class Members via
14 Facebook's private messaging function are and have been at all relevant times electronic
15 communications.

16 110. The conduct alleged herein does not occur while the private message is in storage.
17 Rather, Facebook utilizes each accused device for the purpose of acquiring and manipulating
18 content from the message in the course of the message's transmission.

19 111. Facebook utilized and continues to utilize one or more devices or technology
20 comprised of an electronic, mechanical, or other device or apparatus to intercept the electronic
21 communications transmitted to and from Plaintiffs and Class Members. Such devices or
22 technology include, but are not limited to, web crawlers and social plugins.

23 112. Facebook does not furnish the above-referenced devices or technology to its users,
24 and users do not use the devices for connection to the facilities.

25 113. The intercepting devices or technology are not used for the ability to send or
26 receive electronic communications.

1 114. The devices or technology are not used by Facebook, operating as an electronic
2 communication service, in the ordinary course of business as a provider of an electronic
3 communication service.

4 115. Facebook's interception of electronic communications sent by and to Plaintiffs and
5 Class Members (a) for undisclosed purposes; (b) for the purpose of generating "Likes" for third-
6 party websites; (c) for purposes of providing web traffic data to third parties; (d) for purposes of
7 cataloging user data for targeted advertising and building user profiles; (e) for purposes beyond
8 facilitating private messages sent via Facebook; (f) in violation of its user agreements; (g) in
9 violation of its public statements to users; (h) in violation of federal and California law; and (i) in
10 violation of the property rights of Plaintiffs, Class Members, and third parties. These activities
11 are not within the ordinary course of business of a provider of an electronic communication
12 service.

13 116. Pursuant to 18 U.S.C. § 2511(1)(d), Facebook intentionally used, uses, or
14 endeavored or endeavors to use the contents of Plaintiffs' and Class Members' electronic
15 communications while knowing or having reason to know that it obtained the information through
16 the interception of the electronic communication in violation of 18 U.S.C. § 2511(1)(a).

17 117. Facebook's interception of and use of the contents of Plaintiffs' and Class
18 Members' electronic communications were not performed by an employee engaged in any
19 activity necessary for the rendition of an electronic communication service or for the protection of
20 the rights or property of Facebook.

21 118. Facebook's services that are not related to the ability to send and receive electronic
22 communications are not electronic communication services.

23 119. No party to the electronic communications alleged herein consented to Facebook's
24 interception or use of the contents of the electronic communications.

25 120. Facebook intercepts Plaintiffs' and Class Members' electronic communications for
26 the purpose of committing a criminal or tortious act in violation of the laws of any state, and as
27 such, it cannot obtain consent pursuant to § 2511(2)(d).
28

121. As a result of Facebook's violations of § 2511, pursuant to § 2520, Plaintiffs and the Class Members are entitled to:

a. Preliminary and permanent injunctive relief to require Facebook to fully disclose the extent of its activities, to seek the informed and knowing consent of its users when scanning users' private messages, and to halt Facebook's violations;

b. Appropriate declaratory relief;

c. For Plaintiffs and each Class Member, the greater of \$100 a day for each day of violation or \$10,000; and

d. Reasonable attorney's fees and other litigation costs reasonably incurred.

122. While certain devices and/or technology have been identified in this Complaint, Plaintiffs reserve the right to assert ECPA violations as to any further devices and/or technology disclosed or those devices and/or technology upon which Facebook provides additional information.

COUNT TWO
**(Violations of the California Invasion of Privacy Act,
 Cal. Penal Code §§ 630, *et seq.*)**

123. Plaintiffs adopt and incorporate each and every allegation of this complaint as if stated fully herein.

124. Plaintiffs, individually and on behalf of Class Members, assert violations of the CIPA, Cal. Penal Code §§ 630, *et seq.*, specifically Cal. Penal Code §§ 631(a) and 632, for Facebook's unlawful interception and scanning of the contents of its users' private messages. Facebook uses this information about the sender and recipient for purposes of profiling, marketing, and advertising.

125. Cal. Penal Code § 630 provides that "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."

126. Facebook's acts in violation of the CIPA occurred in the State of California because those acts resulted from business decisions, practices, and operating policies that Facebook developed, implemented, and utilized in the State of California and which are unlawful and constitute criminal conduct in the state of Facebook's residence and principal business operations. Facebook's implementation of its business decisions, practices, and standard ongoing policies that violate the CIPA took place and continue to take place in the State of California. Facebook profited and continues to profit in the State of California as a result of its repeated and systemic violations of the CIPA. Facebook's unlawful conduct, which occurred in the State of California, harmed and continues to harm Plaintiffs and Class Members. Facebook developed, designed, built, and physically placed in California one or more of the accused devices or technology employed by Facebook to violate the CIPA.

127. Plaintiffs and Class Members sent and received private messages, the contents of which included URLs, via Facebook's services.

128. Facebook is not and was not at any time a party to Plaintiffs' and Class Members' private messages.

129. The private messages exchanged among Plaintiffs and Class Members are messages.

130. These messages are communications among Plaintiffs and Class Members.

A. Violations of Cal. Penal Code § 631(a)

131. Pursuant to Cal. Penal Code § 7, Facebook, a corporation, is a "person."

132. Facebook uses a "machine," "instrument," "contrivance," or "in any other manner" is able to, read or to learn the content or meaning of Plaintiffs' and Class Members' private messages.

133. Facebook acts willfully when it reads, attempts to read, or learns the content or meaning of Plaintiffs' and Class Members' private messages.

134. Facebook does not have the consent of any party to the communication, or it acts in an unauthorized manner, when it reads, attempts to read, or learns the content or meaning of Plaintiffs' and Class Members' private messages.

135. Plaintiffs' and Class Members' private messages are "any message, report, or communication."

136. At the time Facebook reads, attempts to read, or learns the content or meaning of Plaintiffs' and Class Members' private messages, the private messages are in transit.

137. At the time Facebook reads, attempts to read, or learns the content or meaning of Plaintiffs' and Class Members' private messages, the private messages are passing over any wire, line, or cable.

138. Private messages – coded, written messages sent electronically to remote locations – are telegraphs within the meaning of the CIPA and this section of CIPA. As such, the wires, lines, cables and/or instruments which carry and facilitate the transmission of Plaintiffs' and Class Members' private messages are telegraph wires, lines, cables and/or instruments within the meaning of the CIPA and CIPA § 631(a).

139. Plaintiffs and Class Members do not consent, expressly or impliedly, to Facebook's eavesdropping upon and recording of their private messages. Facebook does not disclose material information to its users relating to its attempts at, among other things, intercepting, scanning and reading the contents of users' private messages.

140. There is no knowledge or expectation among Plaintiffs and Class Members regarding the extent of Facebook's reading of message content, learning about the content or meaning of users' private messages, the acquisition of such content, the collection of such content, or the manipulation of such content. Each and every one of these actions extends beyond the normal occurrences, requirements, and expectations regarding the facilitation and transmission of Facebook's private messages.

B. Violations of Cal. Penal Code § 632

141. Pursuant to Cal. Penal Code §§ 7 and 632(b), Facebook, a corporation, is a "person."

142. Cal. Penal Code § 632 prohibits eavesdropping upon or the recording of any confidential communication, including those occurring by telephone, telegraph or other device,

1 through the use of an amplification or electronic recording device without the consent of all
2 parties to the communication.

3 143. Facebook intentionally and without the consent of any party to the communication
4 eavesdrops upon and/or records the contents of Plaintiffs' and Class Members' private messages.

5 144. Facebook uses electronic amplifying or recording devices, including its web
6 crawlers and social plugins, to eavesdrop upon and to record Plaintiffs' and Class Members'
7 private messages, for purposes independent and unrelated to storage.

8 145. Plaintiffs' and Class Members' private messages are confidential communications
9 with specifically identified and designated recipients.

10 146. At the time Plaintiffs and Class Members transmit private messages via Facebook,
11 their communications are confidential because the communications are confined to those persons
12 specified as recipients in the destination address fields. There neither would nor could be any
13 expectation that a third party, such as Facebook, would act in any manner other than to facilitate
14 the communication of the private message between the sender and the intended recipient or
15 recipients. There certainly would not and could not be any expectation that Facebook – a third
16 party – would scan the contents of the private message in an effort to catalog and manipulate the
17 information contained therein.

18 147. There is no knowledge or expectation among Plaintiffs and Class Members
19 regarding the extent of Facebook's reading of users' private message content, learning about the
20 content or meaning of the private messages, acquiring and collecting the content of such
21 messages, and manipulating the content of such messages – each action being beyond the normal
22 occurrences, requirements, and expectations regarding the facilitation and transmission of
23 Facebook's private messages.

24 148. Plaintiffs' and Class Members' private messages sent via Facebook are carried on
25 among the parties by means of an electronic device that is not a radio.

26 149. Plaintiffs and Class Members do not consent, expressly or impliedly, to
27 Facebook's eavesdropping upon and recording of their private messages. Facebook does not
28

disclose material information to its users relating to its attempts at reading, scanning, acquiring, collecting, and manipulating the contents of users' private messages.

150. While Plaintiffs have identified certain accused devices and/or technology in this Complaint, Plaintiffs reserve the right to assert violations of Cal. Penal Code §§ 631 and 632 as to any further devices or technology subsequently discovered or any devices or technology upon which Facebook provides additional information.

C. Relief Sought Under Cal. Penal Code § 637.2

151. As a result of Facebook's violations of Cal. Penal Code §§ 631 and 632, Plaintiffs and the Class are entitled to:

a. Preliminary and permanent injunctive relief to require Facebook to fully disclose the extent of its activities, to seek the informed and knowing consent of its users when scanning users' private messages, and to halt Facebook's violations;

b. Appropriate declaratory relief;

c. Monetary relief in the amount set forth in Cal. Penal Code § 637.2(a) for each Class Member; and

d. Reasonable attorney's fees and other litigation costs reasonably incurred.

COUNT THREE

**(Violations of California's Unfair Competition Law
California Business & Professions Code § 17200 et seq.)**

152. Plaintiffs and Class Members reallege and incorporate by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

153. Facebook's conduct as alleged herein constitutes unfair, unlawful, or fraudulent business acts or practices as proscribed by Section 17200, *et seq.*, of the California Business & Professions Code ("UCL").

154. Facebook's conduct constitutes "unlawful" business acts or practices by virtue of Defendant's violation of the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510, *et seq.*, Cal. Penal Code §§ 631(a) and 632.

155. Plaintiffs reasonably relied on Facebook's representations that Plaintiffs' private messages are viewable only by the sender and the recipient, and as a result engaged in "private"

1 messaging on Facebook. Facebook failed to disclose to Plaintiffs and members of the general
2 public that it systematically reviews and captures the content of, and metadata associated with,
3 Plaintiffs' private messages. Facebook failed to disclose that it aggregates the content and data of
4 private messages, using it to sell advertising for a profit. Facebook's Data Use Policy fails to
5 disclose Facebook's acts or practices, and together with its statements that private messages are
6 viewable only by the sender and the recipient, are likely to deceive members of the public. As a
7 result, Facebook's conduct constitutes "fraudulent" business acts or practices.

8 156. Plaintiffs have an interest in controlling the disposition and dissemination of their
9 private messages. Contrary to Plaintiffs' interests, Facebook exercised control over the content of
10 Plaintiffs' private messages, exploiting it for sale and profit without Plaintiffs' consent. As a
11 result, Facebook's conduct constitutes "unfair" business acts or practices.

12 157. Plaintiffs have suffered injury in fact and lost money or property as a result of
13 Facebook's business acts or practices.

14 158. Plaintiffs and Class Members seek an order to enjoin Facebook from such
15 unlawful, unfair, and fraudulent business acts or practices, and to restore to Plaintiffs and Class
16 Members their interest in money or property that may have been acquired by Facebook by means
17 of unfair competition.

18 **JURY DEMANDED**

19 Pursuant to Federal Rule of Civil Procedure 38, Plaintiffs, individually and on behalf of
20 the Class they seek to represent, demand a jury on any issue so triable of right by a jury.

21 **PRAYER FOR RELIEF**

22 WHEREFORE, Plaintiffs, on behalf of themselves and all Class Members, request
23 judgment be entered against Facebook and that the Court grant the following:

24 1. An order determining that this action may be maintained as a class action under
25 Rule 23 of the Federal Rules of Civil Procedure, that Plaintiffs are proper class representatives,
26 that Plaintiffs' attorneys be appointed Class counsel pursuant to Rule 23(g) of the Federal Rules
27 of Civil Procedure, and that Class notice be promptly issued;

1 2. Judgment against Facebook for Plaintiffs' and Class Members' asserted causes of
2 action;

3 3. Appropriate declaratory relief against Facebook;

4 4. Preliminary and permanent injunctive relief against Facebook;

5 5. An award of statutory damages to Plaintiffs and Class Members pursuant to
6 18 U.S.C. § 2520, for each, the greater of \$100 a day for each day of violation of Count One, or
7 \$10,000;

8 6. An award of statutory damages to Plaintiffs and Class Members pursuant to Cal.
9 Penal Code § 637.2, for each, the greater of \$5,000 or three times the amount of actual damages
10 sustained by Plaintiffs and Class Members;

11 7. An award of reasonable attorney's fees and other litigation costs reasonably
12 incurred; and

13 8. Any and all relief to which Plaintiffs and the Class may be entitled.
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

1 Dated: December 30, 2013

LIEFF CABRASER HEIMANN & BERNSTEIN, LLP

2
3 By: /s/ Michael W. Sobol

4 Michael W. Sobol

5 Michael W. Sobol (State Bar No. 194857)

msobol@lchb.com

6 Melissa Gardner (State Bar No. 289096)

mgardner@lchb.com

LIEFF CABRASER HEIMANN & BERNSTEIN, LLP

7 275 Battery Street, 29th Floor

San Francisco, CA 94111-3339

8 Telephone: 415.956.1000

9 Facsimile: 415.956.1008

Rachel Geman

10 rgeman@lchb.com

Nicholas Diamand

11 ndiamand@lchb.com

LIEFF CABRASER HEIMANN & BERNSTEIN, LLP

12 250 Hudson Street, 8th Floor

New York, NY 10013-1413

13 Telephone: 212.355.9500

14 Facsimile: 212.355.9592

Hank Bates (State Bar No. 167688)

15 hbates@cbplaw.com

Allen Carney

16 acarney@cbplaw.com

David Slade

17 dslade@cbplaw.com

CARNEY BATES & PULLIAM, PLLC

18 11311 Arcade Drive

Little Rock, AR 72212

19 Telephone: 501.312.8500

20 Facsimile: 501.312.8505

21 *Attorneys for Plaintiffs and the Proposed Class*