

From: DeMartino, Laura </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=LDEMARTINO>
Sent: Monday, October 21, 2013 5:51 PM
To: Kohm, James A. <JKOHM@ftc.gov>; Mithal, Maneesha <MMITHAL@ftc.gov>
Subject: Chair Correspondence re Facebook
Attach: Chair 14008875 Facebook.pdf; Chair 14008876 Facebook.pdf

Jim and Maneesha, The Chairwoman received two letters concerning FB, which you may have already seen. One from numerous consumer groups asking that we investigate potential FB order violations, and the other is from the National Asian American Coalition, which discusses the order but also broader privacy/COPPA issues as well. (b)(5)

(b)(5)

LD

1400 8875

Federal Trade Commission
Received

SEP 24 2013

September 17, 2013

Edith Ramirez
Chairwoman
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Chairwoman Ramirez

Dear Chairwoman Ramirez:

As organizations concerned about the health and welfare of America's teens, we urge you to protect this vulnerable group from the proposed new Facebook policy on marketing and advertising. Facebook's policy will give it permission to use the name, profile picture, content, and other actions of teens (and all other users) for commercial purposes without compensation. It also requires 13-to-17-year-olds, as a new condition of service, to "represent that at least one of your parents or legal guardians has also agreed to the terms of this section (and the use of your name, profile picture, content, and information) on your behalf." The FTC, which has acknowledged that teens require special privacy safeguards, must act now to limit the ways in which Facebook collects data and engages in targeted marketing directed at adolescents. It should prevent Facebook from imposing unfair terms on teens and their parents that place them in a position of having to say they secured informed, affirmative consent from a parent or guardian.

It is essential, when teens are involved, that the FTC ensure that Facebook is engaged in fair marketing practices, including its terms of service. Facebook has positioned itself to take full commercial advantage of all the social interactions of adolescents on its online platforms, using a myriad of data-enabled marketing techniques little understood by the average user. Facebook is surely aware that teens will have little time to review these proposed changes, or even become knowledgeable about them before their profiles, photos, and social actions automatically become wholesale fodder for commercial use. As you and the commission know, scholarly research has documented the developmental and cognitive vulnerabilities of adolescents. For example, teens are highly influenced by the choices and preferences of their peers, and can often act impulsively. They should not be subjected to the same range of sophisticated ad-targeting practices that Facebook imposes on adults.

We call on the Federal Trade Commission to critically examine and redress these new changes proposed by Facebook. The commission must enforce its 2011 Consent Decree with Facebook to protect the interests of teens.

Cordially,

African American Collaborative Obesity Research Network

American Academy of Child and Adolescent Psychiatry

American Academy of Pediatrics

Benton Foundation

Berkeley Media Studies Group

Campaign for a Commercial-Free Childhood

Center for Digital Democracy

Center for Global Policy Solutions

Center for Media Justice

Center for Science in the Public Interest

Children's Advocacy Institute

Children Now

Consumers Union

Consumer Watchdog

Corporate Accountability International

Pediatrics Now

Prevention Institute

Public Citizen

Public Health Advocacy Institute

Public Health Institute

Media Alliance

Media Literacy Project

Mercy Hospital's Young People's Healthy Heart Program

National Collaboration for Youth

Shaping Youth

United Church of Christ, OC Inc.

Yale Rudd Center for Food Policy and Obesity

cc: Commissioner Julie Brill
Commissioner Maureen K. Ohlhausen
Commissioner Joshua D. Wright



September 17, 2013

Chairwoman Edith Ramirez
Commissioner Julie Brill
Commissioner Maureen Ohlhausen
Commissioner Joshua Wright
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

14008876
Federal Trade Commission
Received

SEP 24 2013

Chairwoman Ramirez

*Asian American Parent and New Immigrant Complaint
Against Facebook's Privacy Intrusions*

Dear Chairwoman Ramirez and Commissioners Brill, Ohlhausen and Wright,

The National Asian American Coalition, which has a DC regulatory office, has frequently met with Chairwoman Ramirez and many recent past and present commissioners on a broad range of consumer issues over which the Federal Trade Commission (FTC) has jurisdiction. We greatly appreciate the attention that Chairwoman Ramirez and other members of the Commission have previously paid to the concerns of the representatives for twenty million Asian Americans.

Today, we file an initial complaint that challenges Facebook's privacy invasions, but seeks a broad range of consumer and teenage protections that the FTC has so far failed to effectively address. We also call to the FTC's attention that an increasingly large number of ten-year-olds are using Facebook despite the prohibitions of any under thirteen having a Facebook account. In fact, an increasing number of even eight-year-olds have figured out how to elude Facebook's efforts, which we believe are sincere, to limit usage only to those thirteen or older.¹

¹ This is, to a lesser degree, still a problem regarding alcohol and cigarette usage and we will seek an opportunity with the FTC to call a meeting with effective high tech companies to address this matter more effectively. This may include input from the regulators addressing teenage usage of cigarettes and alcoholic beverages, such as the Food and Drug Administration. We may also urge progressive elements within the alcohol beverage and tobacco industries join us.

We also call to the FTC's attention that according to a survey of 1,000 parents mentioned in the *Wall Street Journal*, 19% of children age ten have a Facebook account, 32% at the age of eleven and 55% at the age of twelve. We also note that the CEO of Facebook, Mark Zuckerberg, stated that "he believed that children under thirteen should be allowed to use Facebook. That will be a fight we take on at some point." It is also a fight we will take on to protect children under thirteen since there is growing evidence that children ages six and seven are using Facebook. See, for example, consumer reports stating that five million under the age of ten use Facebook.



Facebook's technology is of extraordinary value to Facebook and its shareholders (a market capital valued at over \$106 billion). It is also highly valuable to a presently incalculable degree to the corporations and businesses that rely on Facebook's skilled and sophisticated invasions of privacy.

Although we acknowledge that Facebook has value to its users, we believe, as presently constituted, the net value of Facebook to twenty million Asian Americans may be well below zero given its controversial and disingenuous policies.

As set forth below in this preliminary community advisory letter to the FTC, we believe that the FTC should consult with the only federal consumer agency that has so far shown an ability to address systemic problems, the Consumer Financial Protection Bureau. It should consult to develop appropriate protections and remedies. See, for example, over \$600 million in successful remedies for holders of Capital One, American Express and Discover credit cards.

The standard for evaluating Facebook's policies as they relate to invasions of privacy should, consistent with the U.S. Supreme Court's view of constitutional construction, be viewed in the context of what would be acceptable and what would be expected from pre-Facebook type technologies and/or the development of a universal standard that is appropriate for a nation with diverse backgrounds and educational attainments.

This filing also acknowledges that Facebook is not the only high tech invader of privacy and that similar problems may exist as to, for example, Twitter.

In particular, we call attention to the fact that the majority of Asian American parents are new immigrants born outside the U.S., often in nations that, until very recently, were bypassed by any forms of modern technology. Their children are in many ways inadequately supervised in terms of modern technology, such as Facebook's, since these parents are unfamiliar with the dangers of the technology and are unable to provide their children with any appropriate guidance and standards.

In filing this preliminary notice to the FTC on behalf of Asian Americans, we believe that similar problems confront 90% of parents regarding their teenagers, disproportionately Black and Latino parents and parents who live from paycheck-to-paycheck.

Suggested Actions

Facebook's dealing with users is a wholly unbalanced relationship in which no user has the power and/or the ability to modify Facebook's fundamental policies. Therefore, the FTC's announcement of September 11, 2013 that it has begun an inquiry into whether Facebook's new privacy policies (commenced two weeks ago) violated a 2011 agreement with the regulators, even if properly resolved, will only create a cosmetic change.



Facebook is becoming increasingly powerful through its lobbyists and hundred billion plus market capital. It is therefore in a position to continue, albeit in different forms, similar violations. Obviously, for example, the FTC's continued oversight of its 2011 consent order has not been sufficient.

The National Asian American Coalition, based upon its many years of experience in dealing with, for example, "too big to fail" banks, wishes to recommend far more stringent and effective actions that will put the burden almost exclusively on Facebook rather than parents to protect the privacy of their teenagers. This will also include efforts to effectively bar preteenagers for use of Facebook accounts.

We will also be contending and offering evidence that Facebook's policies present a problem to the vast majority of adults, particularly among the minority community of 130 million and the 70% of Americans who have a job and live from paycheck-to-paycheck.

We are prepared to demonstrate that Facebook, unlike some corporations that introduce new and/or unfamiliar technologies, has a grossly inadequate policy of creating a fully educated user base and/or parental oversight base.

There are many models that FTC can consider, including the equivalent of massive financial education programs presently being administered by many nonprofits relating to consumer and/or housing financial issues. We would, for example, urge that as part of any resolution, Facebook be required to dedicate 2% of its market capital value to massive educational programs dedicated to developing sophisticated users who can effectively address any Facebook invasions of privacy whether deliberate or inadvertent.

The National Asian American Coalition's Next Steps

The National Asian American Coalition will be meeting with the leadership from the 5,000 Black AME churches and the Hispanic evangelical pastors during the week of September 23rd to discuss appropriate actions. Some have already indicated a preliminary interest in joining this letter.

The leadership from Black and Latino churches and the National Asian American Coalition will be seeking a meeting with Chairman Ramirez and other members of the Commission in DC during the week of November 12th, when we will be visiting other regulators, including the Federal Communications Commission, the Food and Drug Administration and the Department of Justice's antitrust division.

The National Asian American Coalition, once it contacts Facebook later this week, will initiate a survey of Asian American, Latino and Black users and potential users of Facebook relating to privacy issues. The first survey may be conducted as early as October 18th at the National Asian American Coalition's Tenth Annual Asian American Economic Development and Empowerment Conference, which will be attended by over 1,000 minority consumers. (See attached program flyer for details of the conference.)




After we contact Facebook, we will contact Chairwoman Ramirez's office to determine whether the FTC would prefer to have direct input into our person-to-person survey that might be conducted on October 18th.

Chairwoman Ramirez and members of the Commission, you have a uniquely difficult task before you. It is a task that an increasingly large number of regulators face. How do you, as a regulator, promote innovation, which we strongly support, while protecting privacy and the financial well-being of the public? We are confident that, once this becomes a priority, other regulators will cooperate and provide input, including the Consumer Financial Protection Bureau.

We will contact your office within ten days to arrange the week of November 12th meetings and to follow up regarding the interests of Facebook in conducting an appropriate survey. We will also contact Twitter and Google as to their interest in joining such a survey.

Most sincerely,


Faith Bautista
President and CEO


Mia Martinez
Chief Deputy


Robert Gnaizda
General Counsel

Cc: Black AME Churches
Ecumenical Center for Black Church Studies
Jesse Miranda Center for Hispanic Leadership
Orange County and San Diego Interdenominational Ministerial Alliances
Los Angeles Latin Business Chamber

Attachment.

NAAAC

Friday, October 18, 2013

11:00 am | Private luncheon with 2013 Awardees James Doty and Bruce C. Berman

2:00 pm | Public Energy and Information Town Hall moderated by CPRE Commissioner Curtis Pittman

3:30 pm | Public Town Hall session with the FCC Chairman, Greg Federal Reserve's San Diego District and Department of Treasury's Mary Miller with Banks, Community Leaders and Customers

5:00 pm | Reception

6:30 pm | Dinner begins

7:00 pm | Awards and Dinner Concludes

Entertainment provided by:



Tracy Albert
Mayor of San Diego



Mariana Sab Shroder
Mayor of San Diego

Awardees

Sarah Bloom Reskin
Federal Reserve Governor

Comerica Bank
Presented to J. Michael Patton

Thomas Curry
Comptroller of the Currency

U.S. Bancorp
Presented to Lisa Glover

Shirley Horton
Former California Assistant Attorney General

Wells Fargo
Presented to Vanessa Hernandez, Jr.

Toulin Thao
Mining Community Leader

JP Morgan Chase
Presented to Eric O'Donnell

Julia Goww
Cali West Bank President and COO

10th ANNIVERSARY AWARDS AND DINNER GALA



Join the National Asian American Coalition in celebrating its Tenth Annual Economic Development and Empowerment Conference at the **Town and Country Resort & Convention Center** located at 500 Hotel Circle North, San Diego, CA 92108 on Friday, October 18, 2013!

This special event will commemorate the past ten years of the National Asian American Coalition and the individuals, corporations, nonprofit institutions and government agencies we have worked with since 2003.

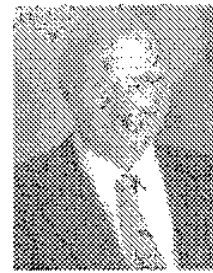
Keynote Speakers



Sarah Bloom Reskin
Federal Reserve Governor



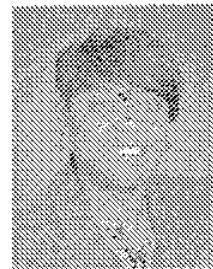
Thomas Curry
Comptroller of the Currency



James Doty
Public Company Accounting Oversight Board Chairman



Mary Miller
Department of Treasury Undersecretary



Carla Petatman
California Public Utilities Commissioner

Partial List of Sponsors

Wells Fargo
Wal-Mart
Verizon
Southern California Edison
JP Morgan Chase
Bank of America
Robertson
HSBC
First Republic
Komenca
HomeLife-USA

Soylent Airlines
East West Bank
Credentia Bank
Promontory Financial Group
AT&T
Cox
U.S. Bancorp
Comcast
Southern California Gas Co.
TDRM
KBC

Asian Journal
Bank of the West
Hawaii Bank
First American
Caltan Bank
Manufacturers Bank
Pacific Western Bank
City National Bank
First Bank
Grandpoint Capital

Registration

web: edc.naacoalition.org

call: 858-537-1500

email: info@naacoalition.org

*** RX REPORT ***

RECEPTION OK

TX/RX NO	5326
RECIPIENT ADDRESS	
DESTINATION ID	
SE. TIME	09/18 09:44
TIME USE	12'52
PGS.	6
RESULT	OK

From: Mithal, Maneesha </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/
CN=MMITHAL>
Sent: Monday, October 21, 2013 9:05 PM
To: Olsen, Christopher <colsen@ftc.gov>
Subject: did you see Asian American letter on Facebook privacy?

From: Kohm, James A. </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/
CN=JKOHM>
Sent: Monday, November 4, 2013 12:05 PM
To: Mithal, Maneesha <MMITHAL@ftc.gov>
Subject: Document1 [Compatibility Mode]
Attach: Document1 [Compatibility Mode].docx

From: Kohm, James A. </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/
CN=JKOHM>
Sent: Thursday, November 14, 2013 1:04 PM
To: Mithal, Maneesha <MMITHAL@ftc.gov>
Subject: Document1 [Compatibility Mode]
Attach: Document1 [Compatibility Mode].docx

From: Jeffrey Chester </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=JEFFREYCHESTER>
Sent: Monday, October 21, 2013 7:48 AM
To: Rich, Jessica L. <JRICH@ftc.gov>; Mithal, Maneesha <MMITHAL@ftc.gov>; jkohn@ftc.gov
Cc: Hudson <hudson@democraticmedia.org>
Subject: Facebook follow-up

Dear Jessica, Manessha and Jim:

I know you are just back to work, but just an FYI that we sent Jessica some follow-up materials, and are ready to provide additional information and analysis.

The market report, which I wrote, reflects just some of the data we have compiled on Fb's operations. I put in citations, but we have other material as well.

We hope the commission continues its review of Fb's proposed ToS/data plan, and ensures that its users--esp. teens--are protected by the consent decree.

Many thanks,

Jeff

Jeffrey Chester
Center for Digital Democracy
1621 Connecticut Ave, NW, Suite 550
Washington, DC 20009
www.democraticmedia.org
www.digitalads.org
202-986-2220

From: Mithal, Maneesha </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/
CN=MMITHAL>
Sent: Wednesday, November 6, 2013 7:56 AM
To: Olsen, Christopher <colsen@ftc.gov>
Subject: Facebook meeting

I made arrangements to go to the FB meeting. You're still welcome to come, but you don't have to.

From: Olsen, Christopher </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/
CN=RECIPIENTS/CN=COLSEN>
Sent: Wednesday, November 6, 2013 4:52 PM
To: Mithal, Maneesha <MMITHAL@ftc.gov>
Subject: FB meeting

I need to drive over to HQ and park because I need to leave right after the FB meeting. So I will just meet you over there.

From: Mithal, Maneesha </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=MMITHAL>
Sent: Thursday, November 14, 2013 6:48 PM
To: Berger, Laura <LBERGER@ftc.gov>; Olsen, Christopher <colsen@ftc.gov>
Subject: Fb meeting

Laura - we can call you on your bb for the meeting. (b)(5)

(b)(5)

From: Mithal, Maneesha </o=FTCEXCHANGE/ou=First Administrative Group/cn=Recipients/cn=MMITHAL>
Sent: Friday, October 18, 2013 3:25 PM
To: Kohm, James A. <JKOHM@ftc.gov>
Subject: FB Q&A

(b)(5)

From: Kohm, James A. </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/
CN=JKOHM>
Sent: Friday, October 18, 2013 4:53 PM
To: Mithal, Maneesha <MMITHAL@ftc.gov>
Subject: FB

(b)(5)

From: Jeffrey Chester </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=JEFFREYCHESTER>
Sent: Tuesday, October 15, 2013 10:19 AM
To: Rich, Jessica L. <JRICH@ftc.gov>; Mithal, Maneesha <MMITHAL@ftc.gov>; Kohm, James A. <JKOHM@ftc.gov>; Koss, Laura <LKOSS@ftc.gov>; Wolfe, Douglas <DWOLFE@ftc.gov>; Kim, Reenah <rkim1@ftc.gov>; Poss, Patricia H. <PPOSS@ftc.gov>; Hasty, Andrew <ahasty@ftc.gov>; Berger, Laura <LBERGER@ftc.gov>
Cc: Hudson <hudson@democraticmedia.org>; Joy Spencer <joyspencer@democraticmedia.org>
Subject: followup docs, Facebook ToS
Attach: Misrepresentations under FTC Order-5-1.pdf; FTCFacebookDataPracticesFinal1013-1-3.pdf

Dear FTC staff:

Needless to say, I hope the commission and the gov't returns to work soon.

At our meeting, we promised to send follow-up information. Attached are two docs from CDD--a legal memo and one on Facebook's marketing practices and data collection.

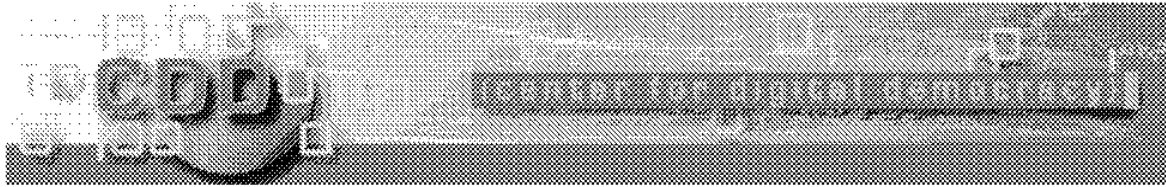
We will contact you after you reopen to discuss a meeting on these issues. Of course, we are happy to provide you with any additional information that could be of assistance.

Many thanks,

Jeff

PS: I do want to also draw your attention to the role of financial data involved with Facebook's data collection/targeting enabled marketing practices (cited in our market analysis). Indeed, due to my research on financial marketing, for a forthcoming report, I was served a payday ad loan on Facebook (delivered via one of Fb's exchange partners). Financial data involves both sensitive information and the need for consumer safeguards. Given the FTC's concern about new financial marketing practices, it is an area that the commission should also focus on as part of its Fb review. We also, of course, believe that adolescents require the same sensitive data safeguards.

Jeffrey Chester
Center for Digital Democracy
1621 Connecticut Ave, NW, Suite 550
Washington, DC 20009
www.democraticmedia.org
www.digitalads.org
202-986-2220



To: Bureau of Consumer Protection, FTC
From: Center for Digital Democracy
Date: October 15, 2013
Re: Misrepresentations by Facebook regarding covered information

I. BACKGROUND

In September 2013 Facebook reached a settlement with a class of users who had sued regarding the company’s use of their images and other content in sponsored stories without properly disclosing the practices. As a result of the deal, Facebook proposed to update its governing documents—called the Statement of Rights and Responsibilities and Data Use Policy—in order to shield itself from similar lawsuits in the future. FTC has ongoing authority to oversee Facebook’s privacy practices under a 2012 Order.

This document seeks to provide more information to the FTC. Specifically, this memorandum provides the agency with information on Facebook’s statements and practices, in order to highlight misrepresentations made in violation of the Order. Other memorandums on Facebook’s data practices and possible other violations of the Order will also be forthcoming.

II. RELEVANT LANGUAGE FROM FTC’S 2012 FACEBOOK ORDER

“Covered information” shall mean information from or about an individual consumer including, but not limited to: (a) a first or last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a mobile or other telephone number; (e) photos and videos; (f) Internet Protocol (“IP”) address, User ID or other persistent identifier; (g) physical location; or (h) any information combined with any of (a) through (g) above. . . .

Decision and Order at 3, In the Matter of Facebook, Inc., Docket No. C-4365 (July 27,

2012).

IT IS ORDERED that Respondent and its representatives, in connection with any product or service, in or affecting commerce, shall not misrepresent in any manner, expressly or by implication, the extent to which it maintains the privacy or security of covered information, including, but not limited to:

- A. its collection or disclosure of any covered information;
- B. the extent to which a consumer can control the privacy of any covered information maintained by Respondent and the steps a consumer must take to implement such controls;
- C. the extent to which Respondent makes or has made covered information accessible to third parties; . . .

Decision and Order at 3-4, In the Matter of Facebook, Inc., Docket No. C-4365 (July 27, 2012).

III. MISREPRESENTATIONS BY FACEBOOK IN VIOLATION OF THE ORDER

Under an agreement with FTC in 2012—Decision and Order, In the Matter of Facebook, Inc.—(“Order”) Facebook is under a broad duty to not “misrepresent in any manner. . . the extent to which it maintains the privacy or security of” users’ “covered information.” Covered information includes all sorts of information that users would consider private and personally identifiable, as well as “any information combined with” listed private and personally identifiable information.

This memorandum covers misrepresentations that offend the Order’s broad statement on misrepresentations, as well as specific subparts of Part I of the Order. Rather than focusing on the legal standard (a broad and straightforward statement about staying truthful) this document seeks to flesh out evidence that the facts are not as Facebook spins them. Recent media and emailed-to-users statements surrounding Facebook’s court-ordered changes to its privacy policy are misrepresentations designed to steer users away from reading the policy documents and understanding what they stand to lose. Statements that the company does not share private information with advertisers misrepresents the ways that Facebook allows advertisers to collect

covered information, either *qua* non-advertisers or through tracking technologies like cookies. Moreover, and in the alternative, Facebook's statements that these changes merely clarify existing policy suggest that the company has been violating users' privacy for a year or more under the Order. FTC must further investigate these violations and seek accountability.

A. The "no change" misrepresentation: violating the "misrepresent in any manner" broad language of Part I's introductory paragraph

Facebook's assurances that it is only clarifying its existing policy is not borne out by the facts, and this repeated refrain would cause normal users to avoid investigating the changes made by the company. This violates the language in the first paragraph of Part I of the Order.

On September 12, 2013, the Washington Post quoted Jodi Seth, Facebook spokesperson in an official statement: "Importantly, our updated policies do not grant Facebook any additional rights to use consumer information in advertising. Rather, the new policies further clarify and explain our existing practices."¹ This statement has been widely reported² and is likely one of the largest-bore statements on the Facebook policy change because it spread in the media, as opposed to other statements buried in Facebook's many policy pages. This statement would lead a normal user to believe that there is no change in the company's rights to use their Facebook information in advertisements.

The proposed policy changes were made as part of a settlement where plaintiffs alleged Facebook's improper use of consumer information in advertising.³ The plaintiffs alleged

¹ Hayley Tsukayama, *FTC evaluating Facebook policy changes*, Washington Post, Sept. 12, 2013, http://www.washingtonpost.com/business/technology/ftc-evaluating-facebook-policy-changes/2013/09/11/da1db8ba-1b3f-11e3-8685-5021e0c41964_story.html.

² A google search on September 18, 2013, reveals that this exact quote was also used in stories in CNET, The Wall Street Journal, NBC News's online blog, NPR, and a host of lesser-known industry and news sites.

³ CGC, *Fralely v. Facebook, Inc.*, <http://www.fralelyfacebooksettlement.com> (last visited Sept. 30, 2013).

numerous violations of California law, and the fact that Facebook's privacy policy did not disclose clearly how it used user data. Though the company did not admit fault in the settlement, the nonmonetary conditions require Facebook to make substantive changes in its official policy regarding how the company intends to use user's information in sponsored stories⁴ and change the legal rights of minor users in relation to the company's unannounced and uncompensated use of their information in advertisements.⁵ These changes are reflected in the new document, and as discussed in this section and below (*infra* at C) they change and expand Facebook's rights to use more types of information from user profiles in commercial messages.

To say that the changes do not expand Facebook's claims to user information is to ignore the purpose of the settlement's requirements to express what Facebook did not state prior to the underlying lawsuit. Stated another way: there would have been no lawsuit and no binding settlement of the same if there is actually "no change" in Facebook's policy related to user data in advertisements.

Moreover, the company's own summary of the changes makes clear that most of them are substantive (noting in a summary of the changes that there are a few "non-substantive

⁴ CGC, *Fraley v. Facebook, Inc.*, Frequently Asked Questions: Question 7, <http://www.fraleyfacebooksettlement.com/faq#Q7> (last visited Sept. 30, 2013) (for example, it is bound to: "Revise its terms of service (known as the "Statement of Rights and Responsibilities") to more fully explain the instances in which Class Members agree to the display of their names and profile pictures in connection with Sponsored Stories.").

⁵ CGC, *Fraley v. Facebook, Inc.*, Frequently Asked Questions: Question 7, <http://www.fraleyfacebooksettlement.com/faq#Q7> (last visited Sept. 30, 2013) ("Revise its terms of service to confirm that Minor Subclass Members represent that their parent or legal guardian consents to the use of their names and profile pictures in connection with commercial, sponsored, or related content.").

grammatical corrections” in addition to the many other changes highlighted in the bulk of the summary).⁶

Misrepresentation particularly pernicious when in regards to parents’ right to consent

One change in the new policies alters the legal rights of a whole community of Facebook users. In the proposed new text there is a wholly new paragraph on the legal status of minors:

If you are under the age of eighteen (18), or under any other applicable age of majority, you represent that at least one of your parents or legal guardians has also agreed to the terms of this section (and the use of your name, profile picture, content, and information) on your behalf.⁷

As can be seen from the current Statement of Rights and Responsibilities,⁸ there was no statement about minor’s representations prior to this change. Minors are not allowed to enter into this type of contract under applicable state law. California Family Code § 6701 forbids contracts where minors delegate power, or contracts affecting the minor’s personal property not in the minor’s possession.⁹ The appropriation of children’s content, information, and images seemingly would be a delegation and the company’s retention of user information means that this property is not held by the users themselves—both provisions are therefore violated when Facebook essentially contracts with children without any parental oversight. Under state law these contracts are not voidable, they are forbidden.¹⁰

⁶ Facebook, Section-by-Section Summary of Updates <http://www.facebook.com/notes/facebook-site-governance/section-by-section-summary-of-updates/10153200989785301> (last visited Sept. 30, 2013).

⁷ Facebook, Proposed Statement of Rights and Responsibilities Redline 6 (Sept. 2013), https://fbcdn-dragon-a.akamaihd.net/hphotos-ak-prn1/851575_209563965879553_209116475_n.pdf.

⁸ See *id.* (showing the existing policy in non-redline portions of the PDF); Facebook, Statement of Rights and Responsibilities (Dec. 11, 2012) <https://www.facebook.com/legal/terms>.

⁹ CAL. FAM. CODE § 6701(a)&(c). See also *Fraley v. Facebook*, Case No. CV 11-01726 RS, *Amicus* brief by Center for Public Interest Law and Children’s Advocacy Institute, Document 248 Filed 11/07/12 (N.D. Cal. Nov. 15, 2013) (discussing the California Family Code and how the settlement changes parents’ rights and children’s protections under state law).

¹⁰ See CAL. FAM. CODE § 6701.

Hence, according to the law applying to the pre-amendment Facebook policies, minors could not legally give up their images or other Facebook content for commercial uses; under the proposed change, minors effectively give up all of their content for Facebook's profit. This harms children's free speech interests as well as their privacy and their parents' right to oversee use of their images in commercial statements. Indeed, as one party opposing the underlying settlement argues, this attempt to circumvent parental consent is expressly against the law of seven states.¹¹

Because minors are protected from having their image misappropriated for commercial uses without parental consent under numerous states' laws, this is a large departure. Under the existing policy Facebook had no argument under which it could use minors in sponsored stories and therefore would have to ask for parental consent to use minors' content in this way, now its policy says it never has to ask for further parental consent for the same. This is a sea change, a major expansion in the company's assertion of its rights to use minors' information.

Statements that there are no significant changes to Facebook's policies are misrepresentations of Facebook's protection of user privacy in violation of the Order, and they are dangerous to parent and child rights under state law.

¹¹ Press Release, Public Citizen Appeals Settlement That Allows Facebook To Violate Minors' Privacy Rights (Sept. 24, 2013), <http://www.citizen.org/pressroom/pressroomredirect.cfm?ID=3985>. This violates laws in California, Florida, New York, Oklahoma, Tennessee, Virginia and Wisconsin. *Id. See also* Fraley v. Facebook, Case No. CV 11-01726 RS, Public Citizen's Objection to Proposed Settlement and Notice of Intent to Appear (June 28, 2013) (discussing the seven state laws more fully), available at <http://www.citizen.org/documents/Fraley-v-Facebook-Objection.pdf>.

B. The “your information is safe from advertisers” misrepresentation: violating subparts A, B, and C of Part I of the Order¹²

Facebook’s past and future policies would lead users to believe that the company does not share their covered information with advertisers without explicit informed consent, however in practice the company does just that. These misrepresentations undercut users’ ability to see how porous the Facebook privacy wall remains.

In an email message announcing the policy changes, sent by Facebook’s Chief Privacy Officer, the text echoes the above idea that these are routine and unimportant changes before going one step further: “Like always, we won’t share the private information that you put on Facebook with advertisers without your permission.”¹³ This statement is repeated in the current Statement of Rights and Responsibilities and partially echoed in the proposed Data Use Policy.¹⁴ This should mean that users are empowered to deny the sharing of their covered information with third party advertisers.

Though this email also contained links to the revised language to Facebook’s policies and a short summary of the changes, it made no reference to Facebook’s position that much covered information, as defined in the 2012 Order, is deemed not “private information” and therefore

¹² This misrepresentation has been Facebook’s position for some time and this section therefore describes a misrepresentation that is not dependent on Facebook’s recent policy change, although it has been repeated in that context.

¹³ E-mail from Erin Egan, Facebook Chief Privacy Officer, to all Facebook users, “News from Facebook” (Aug. 30, 2013 10:52pm EST) (on file with author). That statement is also part of Facebook’s Statement of Rights and Responsibilities in both the existing and proposed versions (i.e. “We do not give your content or information to advertisers without your consent.” see quoted section in C, *infra*).

¹⁴ Facebook, Statement of Rights and Responsibilities (Dec. 11, 2012) <https://www.facebook.com/legal/terms> (“We do not give your content or information to advertisers without your consent.”); Facebook, Proposed Data Use Policy Redline 15 (Sept. 2013), https://fbcdn-dragon-a.akamaihd.net/hphotos-ak-prn1/851585_445264755581605_1677569786_n.pdf (“When we deliver ads, we do not share your information (information that personally identifies you, such as your name or contact information) with advertisers unless you give us permission.”).

cannot be said to be within the user's power to restrict sharing. In the Data Use Policy and elsewhere on Facebook's website it outlines what it considers to be "public information," including: any information a user shares and leaves the privacy setting on that item as "public;" any comment or post that a user adds to Facebook where the user is not given an option to toggle the audience; user's real name; profile picture; cover photo; network (i.e. networks associated with one's alma mater or work); gender; user name and User ID.¹⁵ This information allows users to be searched for and associated with other information both on and off Facebook.¹⁶ Facebook's only offered control on the general dissemination of this information is users' deletion of their accounts.¹⁷ Hence, the user "permission" and control that Facebook flaunts is often an unknown default setting allowing Facebook to share covered information with any and all other internet users. In respect to Facebook's partners, and applications, which might also be advertisers on Facebook, the company also provides a user's full friend list as part of the "basic information" that is shared as a matter of course.¹⁸

¹⁵ Facebook, Information we receive about you, Public Information, <https://www.facebook.com/about/privacy/your-info#public-info> (last visited Sept. 30, 2013). The hyperlink in the email to "Privacy" lead not to this official policy about privacy information, but rather to a forum where users could "like" and discuss Facebook privacy. See Facebook and Privacy, <https://www.facebook.com/lbprivacy> (last visited Sept. 30, 2013).

¹⁶ Facebook, Information we receive about you, Public Information, <https://www.facebook.com/about/privacy/your-info#public-info> (last visited Sept. 30, 2013). Facebook is making large strides in making this information easier to search and is deploying these search capabilities to developers, i.e. internet companies who are marketing to users. See Facebook, Graph API, Getting Started, <https://developers.facebook.com/docs/reference/api/> (last visited Sept. 30, 2013).

¹⁷ Facebook, Information we receive about you, Public Information, <https://www.facebook.com/about/privacy/your-info#public-info> (last visited Sept. 30, 2013) ("If you are uncomfortable sharing your real name, you can always delete your account.").

¹⁸ See, e.g., Facebook, Other Websites and Applications, <https://www.facebook.com/about/privacy/your-info-on-other> (last visited Sept. 30, 2013) ("When you connect with a game, application or website . . . we give the game, application, or website . . . your basic info . . . which includes your User ID and your public information. We also give them your friends' User IDs (also called your friend list) as part of your basic info.").

It is significant that Facebook cautions users that “information you share on Facebook can be copied or re-shared by anyone who can see it”¹⁹ and yet it still confidently claims it does not share information with advertisers (who glean covered information while wearing non-advertiser hats). In contrast, a Facebook partner explains that companies can use Facebook User IDs they have gathered to target individuals on Facebook and encourage them to become “fans,”²⁰ which would open the individuals up to companies’ personally-identifiable-information gathering as “third parties” (rather than as “advertisers”) under Facebook’s construction of the term. Facebook states that when any person searches Facebook using a user’s contact information, Facebook will allow them access to public information, even if a user has not shared the searched-for contact information publicly.²¹ The internal contradictions between the advertiser anonymity statements and other statements, shows how the left hand doesn’t know what the right is doing—users who rely on the most prominent statements about privacy, provided by Facebook’s most prominent spokespeople, will be misled.²²

Accord Facebook, Data Use Policy (Dec. 11, 2012), https://www.facebook.com/full_data_use_policy.

¹⁹ Facebook, Data Use Policy (Dec. 11, 2012), https://www.facebook.com/full_data_use_policy.

²⁰ See Experian Marketing Services, Retargeting on Facebook, <http://www.experian.com/social-marketing/retargeting.html> (last visited Sept. 30, 2013).

²¹ Facebook, Data Use Policy (Dec. 11, 2012), https://www.facebook.com/full_data_use_policy (“we allow anyone with your contact information (such as email address or telephone number) to find you through the Facebook search bar at the top of most pages, as well as other tools we provide, such as contact importers - even if you have not shared your contact information with them on Facebook.”).

²² Even the full Data Use Policy, which admits to some of the uses that contradict other statements about information being safe from advertisers, is hidden to some degree. When one searches for and finds a “Facebook Data Use Policy” page the full policy is discreetly put as a link at the left of the screen, a last option after eight other links (when reading the page right-to-left and top-to-bottom) that would lead away from the policy. See Facebook, Data Use Policy, <https://www.facebook.com/about/privacy/> (last visited Sept. 30, 2013).

Cookies and persistent identifiers

The company's cookie policy is of great importance to Facebook's misrepresentations about user privacy. Under the Order persistent identifiers are covered information. Though Facebook's official stance is that it doesn't share generally-available information with advertisers without user permission, its policies allow it to give advertisers enough information to link covered personal information it deems "public information" with other identifiers.

Facebook and its advertisers track users using cookies and similar technologies.²³ Cookies allow Facebook and third parties "know who you are,"²⁴ and track you from spaces that Facebook controls to non-Facebook-controlled sites that link a user to personally identifiable information.²⁵ In fact, away from its privacy policies, Facebook discusses how it helps third party sites to collapse a user's Facebook profile and profiles on the other sites.²⁶ Merely "liking" a company's Facebook page (many such pages existing for commercial marketing purposes)

²³ Facebook, Advertising on Facebook <https://www.facebook.com/about/ads/#> (last visited Sept. 30, 2013) ("Facebook and other companies use technologies like cookies, pixel tags and local storage to show ads that are relevant to you.").

²⁴ Facebook, Cookies, Pixels & Similar Technologies, <https://www.facebook.com/help/cookies> (last visited Sept. 30, 2013). *See also* Facebook, Data Use Policy (Dec. 11, 2012), https://www.facebook.com/full_data_use_policy ("We may ask advertisers or other partners to serve ads or services to computers, mobile phones or other devices, which may use a cookie, pixel or other similar technology placed by Facebook or the third party").

²⁵ Facebook, Cookies, Pixels & Similar Technologies, <https://www.facebook.com/help/cookies> (last visited Sept. 30, 2013) ("We may also use a cookie to learn whether someone who saw an ad on Facebook later visited the advertiser's site. Similarly, our partners may use a cookie or another similar technology to determine whether we've shown an ad and how it performed or provide us with information about how you interact with them. We also may work with a partner to show you an ad on or off Facebook, such as after you've visited the partner's site or app and this may involve the use of cookies, local storage on your device or other similar technologies.").

²⁶ Facebook, Other Websites and Applications, <https://www.facebook.com/about/privacy/your-info-on-other> (last visited Sept. 30, 2013) ("The website sends over a hashed version of your email address, and we match it with a database of email addresses that we have also hashed. If there is a match, then we tell the website the User ID associated with the email address. This way, when you log into the website using Facebook, the website can link your Facebook account to your account on that website.").

opens a user up to tracking and information collection by that company through Facebook's platform,²⁷ which potentially links user "public information" to data the company gathered from other sources.

Facebook acknowledges that its partners and other third parties are collecting information about its users, but then the company seemingly tries to pass them the liability by pointing its users to these third parties' privacy policies.²⁸ This further undercuts its statements about how it respects users' privacy settings because it is demonstrating that its policy documents do not cover users as they use the Facebook platform. In the context of Facebook's broader statements about respecting privacy this shifting of responsibility is misleading. Additionally, the more one goes digging into materials about partners, advertisers, and third parties, the more shocking the revelations are. For the sake of brevity in this analysis, examples for further FTC investigation are provided in an accompanying Center for Digital Democracy working paper.

This "use at your own risk" stance in terms of identification by third parties and linkage between identifying cookies and covered information is not fairly alluded to in Facebook's statements about advertisers in its email to members and the Statement of Rights and Responsibilities. Widely-reported examples are few (because most users cannot track misuse of their information in an online and personalized advertising platform) but clearly advertisers are

²⁷ Facebook, Data Use Policy (Dec. 11, 2012), https://www.facebook.com/full_data_use_policy ("Some Pages contain content that comes directly from the Page owner. . . . Because this content comes directly from the Page owner, that Page may be able to collect information about you, just like any website.").

²⁸ Facebook, Cookies, Pixels & Similar Technologies, <https://www.facebook.com/help/cookies> (last visited Sept. 30, 2013) ("We or others (like your friends in their posts or the Pages or Apps you visit or use) may integrate third party features like maps or videos to provide you with better services. The providers of those integrations may collect information when you view or use them, including information about you and your device or browser. They may do this using cookies, pixels, or other similar technologies. To learn more about the information they collect or receive, review their privacy policies.").

already using available information from Facebook to create commercial content that violates individual privacy.²⁹

Facebook's many assertions that it does not provide advertisers with information is at odds with its policy of making some sensitive information covered in the 2012 Order generally available and allowing linkage with cookies and similar technologies. Users have little idea to what extent they are being tracked and current policy statements would not give them any meaningful information about Facebook's advertising privacy practices and the holes companies can glean information through.

C. The past policy misrepresentation: violating subparts B and C of Part I of the Order

If Facebook is taken at its word, it has been misleading users the whole time the Order has been in effect. Facebook would lead consumers and FTC to believe that the new expression of its privacy policies is merely a clarification of the existing statements, which in no way expands the scope of potential data gathering and use (*see* statements discussed in A, above). To the extent that the changes are merely clarifications of existing policy, then the complaints raised by class members who settled with Facebook in the *Fraleigh* case show the large extent to which prior policies were inaccurate.

Assuming for a moment that this "clarification" statement is true, then the original unclarified policy statements were misleading to begin with. This is evidenced by Facebook's redline document, which shows changes that appear to be substantive. The advertising section of the Statement of Rights and Responsibilities states:

²⁹ Heather Saul, *Facebook apologises over dating ad showing picture of Rehtaeh Parsons after she killed herself*, THE INDEPENDENT (UK), Sept. 18, 2013, <http://www.independent.co.uk/news/world/americas/facebook-apologises-over-dating-ad-showing-picture-of-rehtaeh-parsons-after-she-killed-herself-8824232.html>.

10. About Advertisements and Other Commercial Content Served or Enhanced by Facebook

Our goal is to deliver advertising and other commercial or sponsored content that ~~we~~ is valuable to our users and advertisers. In order to help us do that, you agree to the following:

1. ~~You can use your privacy settings to limit how your name and profile picture may be associated with commercial, sponsored, or related content (such as a brand you like) served or enhanced by us.~~ You give us permission to use your name, ~~and~~ profile picture, content, and information in connection with commercial, sponsored, or related ~~that~~ content (such as a brand you like) served or enhanced by us, ~~subject to the limits you place.~~ This means, for example, that you permit a business or other entity to pay us to display your name and/or profile picture with your content or information, without any compensation to you. If you have selected a specific audience for your content or information, we will respect your choice when we use it.

If you are under the age of eighteen (18), or under any other applicable age of majority, you represent that at least one of your parents or legal guardians has also agreed to the terms of this section (and the use of your name, profile picture, content, and information) on your behalf.

2. We do not give your content or information to advertisers without your consent.
3. You understand that we may not always identify paid services and communications as such.

As discussed above, the new paragraph on minors is a large change in the company's stance towards a particular group of users, but that is not the only significant revision. Gone is the assurance that one can "limit how your name and profile picture may be associated with commercial, sponsored, or related content," as well as another statement that this information is only used with sponsored content "subject to the limits you place." Instead, there is now blanket permission for Facebook to use both name and profile picture for any sponsored advertisement. This contradicts the previous controls given to users to limit the use of "social actions" in

Facebook ads.³⁰ Moreover, the addition of “content, and information” to the general permission greatly expands the types of user information that could be tied up into an advertisement without a user’s knowledge.

A user who read the Statement of Rights and Responsibilities in 2012 or early 2013 would have no indication that minors were representing their parents had given consent, would not have expected their “content, and information” to be used in commercial messages, and would have assumed they could limit their name and profile picture’s use in sponsored content. According to Facebook’s stance today, that user’s expectations were wrong.

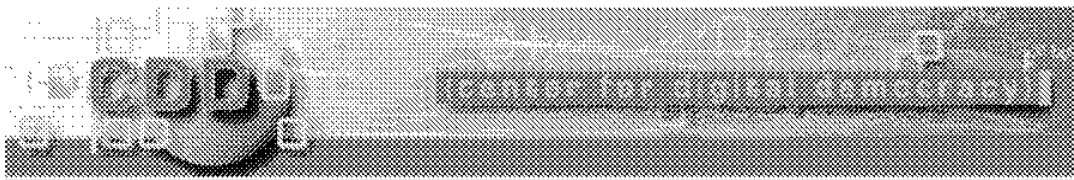
To the extent that Facebook indicates this wholesale use of all user content for commercial messages that goes unnoticed and uncompensated was already its policy, this policy was not reflected in the previous—seemingly more protective—language. Taken at its word, the company has violated subparts I.B. and I.C. of the Order for the entire time this has secretly been Facebook’s *de facto* policy.

By contrast, and more likely still, this is an expansion of the privacy policy’s coverage (as covered *supra* in A) and so Facebook is currently misrepresenting what the document meant in the past. The company’s insistence that there a lack of meaningful change indicates that it is either misrepresenting one policy or the other—and in either case FTC has cause to act under the 2012 Order.

IV. CONCLUSION

For the foregoing reasons FTC should scrutinize Facebook’s misrepresentations of its privacy protections in violation of the order and punish the company accordingly.

³⁰ See Facebook, Proposed Data Use Policy Redline 19 (Sept. 2013), https://fbcdn-dragon-a.akamaihd.net/hphotos-ak-prn1/851585_445264755581605_1677569786_n.pdf (deleting a reference to “Your ‘Show my social actions in Facebook Ads’ setting” to allow for the unlimited use of this information in ads).



Facebook's Misleading Data and Marketing Policies and Practices
Center for Digital Democracy
October 2013

I. Introduction

Facebook makes markedly different—at times completely opposite—statements to advertisers than they do to users about the type of data they make available to marketers. To users, for example, Facebook states that it will not share or “give your content or information to advertisers without your consent.” In practice, however, Facebook does give advertisers user information by matching, linking, hashing, reverse engineering, and creating new IDs that are specific to individuals and persist beyond the Facebook platform. Facebook gives advertisers access to these new IDs, allowing them to follow specific individual users and tie their own external data to these IDs. This allows advertisers to expand their knowledge of specific Facebook users. By creating a parallel system of personal identification, Facebook not only shares data by matching, linking, and tying covered information but they share data that are personally identifiable.

Facebook also claims that it has instituted a system where users can opt out of this marketing and data collection. However, in practice this is an extremely convoluted and misleading process, consisting of multiple steps buried within the Facebook platform. There is no simple way for a user to opt out of this extensive data collection or targeted marketing based on tracking. A user must visit each third-party website individually to actually be informed about its data collection practices (and even then the opt-outs are cookie-based, so any clearing of browser cookies essentially opts the user back into the system).

While this creation and matching of persistent personal IDs have become common data and marketing practices for Facebook, very few consumers have any level of understanding of how this process operates and its implications for privacy. The Federal Trade Commission should address the practices we discuss below, as part of its review on the proposed Data Use policy changes.

II. Sharing User Information: Matching and Tying Covered information through the Facebook Exchange, Partner Categories, and Custom Audiences.

Facebook's Main Advertising and Retargeting Platforms

Facebook Exchange (FBX) is Facebook's real-time bidding platform. You must be a qualified company to be a part of the exchange that currently boasts 20 approved data gathering and targeting companies. Among them are AdRoll, AppNexus, Criteo, and Media Math. FBX allows companies to follow visitors from their websites or across the

Internet back to Facebook for retargeted advertising. Custom Audiences is the mechanism by which Facebook allows marketers to reach their offline audiences among Facebook users “using email addresses, phone numbers, Facebook user IDs or app user ID’s to make the match”¹

Last April 2013, Facebook announced Partner Categories, which offers marketers a self-serve mechanism for targeting their customers.² It helps marketers target users based not only on their expressed interests but also on actions they have taken across the Internet regardless of device. Marketers using this platform have access to offline data from data brokerage companies Acxiom, Datalogix, and Epsilon.³ The 500-plus unique group categories are available to marketers through Power Editor and the API.⁴

In a privacy-related post called “Advertising and our Third-Party Partners,” Facebook describes its new relationship with leading data broker companies as “partnerships [designed] with people’s privacy in mind and how people using Facebook continue to have control over the ads they see.”⁵ The blog explains that Facebook’s work with Acxiom, for example, is innocuous, beneficial, and reflects current business practices used by others: “Many businesses today work with third parties such as Acxiom, Datalogix, and Epsilon to help manage and understand their marketing efforts. For example, an auto dealer may want to customize an offer to people who are likely to be in the market for a new car. The dealer also might want to send offers, like discounts for service, to customers that have purchased a car from them. To do this, the auto dealer works with a third-party company to identify and reach those customers with the right offer.”⁶

On a page discussing “Third-party service providers” Facebook states that “[w]e may work with others to combine information we have collected from you with info provided by an advertiser, to enable the advertiser to send you relevant advertising.”⁷ In a page for marketers, Facebook explains the service differently:

¹ <https://www.facebook.com/help/341425252616329>; <http://www.facebook-pmdecenter.com/fbx>

² <https://www.facebook-studio.com/news/item/partner-categories-a-new-self-serve-targeting-feature>

³ <https://www.facebook-studio.com/news/item/partner-categories-a-new-self-serve-targeting-feature>; <http://www.facebook-pmdecenter.com/fbx>; <http://blog.adespresso.com/facebook-partner-categories-guide/>

⁴ <https://www.facebook.com/help/194355723944655/>

⁵ <https://www.facebook.com/notes/facebook-and-privacy/advertising-and-our-third-party-partners/532721576777729>

⁶ <https://www.facebook.com/notes/facebook-and-privacy/advertising-and-our-third-party-partners/532721576777729>

⁷ <https://www.facebook.com/notes/facebook-and-privacy/targeting-and-our-third-party-partners/532721576777729>; <https://www.facebook.com/help/133547810119620>

To date, advertisers have been able to show ads to people based on their expressed interests on Facebook. Now with partner categories, they can also show ads to people on Facebook based on the products and brands they buy across both desktop and mobile,

Partner categories uses data from select third parties including Acxiom, Datalogix, and Epsilon. No personal information is shared between Facebook, third parties or advertisers. Partner categories work the same way all targeting on Facebook works. The advertiser only knows the size of the audience and can't access any information about individuals included in a category.⁸

Facebook explains Partner Categories to its ad clients this way in its Help Center: "Partner categories are a way to identify and reach the right people with the right message on Facebook, based on their activity off of Facebook. For example, you can use these targeting options to show your ads to people who are heavy buyers of health and wellness products, or who have taken actions that indicate they may be shopping for a new car."⁹ Also in the Help Center it goes on to say "you can use partner categories with other Facebook targeting options" as well as, "We've built partner categories with our partners using their U.S. records."¹⁰

Leveraging Offsite and Facebook User Information for Persistent Identification and Failure to Provide Effective Tools to Address User Privacy

Facebook's "Bring Your Own Data" concept is central to the tying of covered information to vast amounts of data off of Facebook, allowing its advertisers and data partners to leverage as much private information as possible on individual users. Users do not have access to the information about what's collected and how it really works on the Exchange, despite Facebook's claims to the contrary. For example, a review on the partner websites reveals that "[w]ith FBX, Facebook has enabled marketers to import their own customer & intent data Facebook allows each marketer to 'Bring Your Own Data.' If a shopper has shown strong interest in a particular pair of Jimmy Choos on Nordstrom, we can show precisely that user exactly that pair of shoes. Both ad creative and bid pricing decisions are made at the level of the individual user, in real time."¹¹

A Facebook user would have to review closely what Facebook says about each of its providers (i.e., click on "view profile" in their listing), and also analyze what the partner

⁸ <https://www.facebook-studio.com/news/item/partner-categories-a-new-self-serve-targeting-feature>

⁹ <https://www.facebook.com/help/459892990722543/>;
<https://www.facebook.com/help/353223368111533>

¹⁰ <https://www.facebook.com/help/459892990722543/>;
<https://www.facebook.com/help/357737337665825>

¹¹ [http://tellingpart.com/early-results-from-facebook-exchange-show-strong-roi](http://tellingpart.com/early-results-from-facebook-exchange-show-strong-roi;);
<http://tellingparteng.tumblr.com/post/49819416852/early-results-facebook-exchange>

company says on its own site in order to have even a limited understanding of how the two companies work together to track that user.¹² Looking only at Facebook's descriptions misleads a reasonable reader. Facebook's site for Turn, for example, tells users that "Turn delivers real-time insights that transform the way leading advertising agencies and marketers make decisions."¹³ It also cryptically identifies that Turn is involved in "financial services" marketing.¹⁴ But when one goes to Turn's Facebook-related marketing page, the picture it portrays about how it uses user data is much different: "Turn Campaign Suite now enables you to perform custom audience targeting on Facebook, where consumers spend more time than anywhere else on the web. ... [T]o run your Facebook Exchange advertising, you can use the same data sources and sophisticated audience designs for behavioral targeting, demographic targeting, and remarketing as you do for video, mobile, and other display inventory."¹⁵ Essentially, Turn enables companies with existing data on users to target them *individually* on the Facebook platform. The FTC needs to examine, in terms of privacy, what user-related information Turn receives from Facebook and what is also shared with its clients and partners.¹⁶

Facebook is working with financial advertisers that have privacy and consumer protection consequences for users. As one report concerning a recent presentation to the ABA by Facebook's head of global marketing for financial services, Neil Hiltz, explained, "You don't have to tell Facebook what financial products this pool of people has or doesn't have—they don't care. All Facebook needs to know is that you've identified a type of consumer you'd like to focus on. Facebook uses your list to find users in its system attached to the email addresses and phone numbers you've supplied. Facebook can then build a profile of other users who match the "digital account holder" segment you've defined. And Hiltz says you can do this with astonishing precision. "Facebook ads are 90% accurate with our native targeting products — using geo, demo, interest, smartphone, etc., as variables. We can layer this targeting with the bank's data to gain even more efficiency," Hiltz explains. "The 'match rates' between the bank data tables and Facebook audience tables are contingent upon the quality of the bank's dataset,"

¹² See <http://www.facebook-pmdcenter.com/fbx>

¹³ <http://www.facebook-pmdcenter.com/profiles/view/11093>

¹⁴ <http://www.facebook-pmdcenter.com/profiles/view/11093>

¹⁵ <http://www.turn.com/solutions/advertising/facebook-advertising>;
<http://www.turn.com/casestudies/turn-campaign-suite-delivers-strong-roi-financial-services-advertiser>; For an overview of the data tools Facebook makes available to advertisers and marketers, see its "Power Editor" feature for developers: <https://www.facebook.com/help/194355723944655/>. It is important for the commission to address that many of Facebook's exchange data partners are engaged in financial marketing. Through links at Power Editor one accesses developer and advertiser data sheets on Facebook products, such as "Custom Audiences: Creation & Management," "Sponsored Results."

¹⁶ The commission should also investigate how Facebook's data partners gather other data. For example, Turn has far-reaching relationships with numerous data providers that use offline and online data. They include many companies involved in financial services marketing, including Acxiom, Alliant, Epsilon, and MasterCard. <http://www.turn.com/en-gb/data-partners>

Hiltz continues. “We can also work with trusted third-party data providers. We have existing relationships with Acxiom, Epsilon, and DataLogix, and are signing up even more data providers going ...”¹⁷

Adroll’s work also illustrates how Facebook’s claims that users’ identity isn’t shared with advertisers are imprecise—if not disingenuous. The goal of Facebook retargeting (to “serve ads to potential customers who’ve previously visited their website as they browse the web and Facebook,” according to AdRoll) is to bring them back to the marketer’s site—a tactic designed to collect further data from a user.¹⁸ When Facebook facilitates retargeting it is implicitly misleading users whom it has told it would not share their information with advertisers.¹⁹ Facebook also doesn’t explain to users the impact on their financial privacy of data partner AdRoll’s focus on “financial services.”²⁰ Facebook is also working with online lead generation companies—which collect information on users without meaningful disclosure and sell it to loan and other financial companies that often prey on consumers—to help them target its users. As one lead generator using Facebook explained they “can take offline data, such as email addresses or phone numbers, from an advertiser’s CRM or other sources, and find those users on Facebook. ... [W]ith custom audiences we’re able to expand our online targeting to users we historically were unable to identify online ... For a company like DoublePositive, who works with millions of email addresses and phone numbers, this one is huge.”²¹

One would not learn much of anything about one’s data privacy from Facebook’s description of data partner Appnexus.²² If a Facebook user concerned about privacy went to the Appnexus site, he or she might discover that Appnexus uses a broad range of data gleaned from many other companies for its targeting, which can be brought into the Facebook Exchange system by the company.²³ For example, it has relationships with Bluekai, eXelate, Liveramp, Lotame, Neustar, Proxemic, and many more.²⁴ Similarly, a Facebook user eventually finding Criteo on Facebook’s site would learn that it is “user centric and relies on product level recommendation algorithms able to select the right banner at the right time.”²⁵ Should an abnormally diligent Facebook user read Criteo’s

¹⁷ <http://thefinancialbrand.com/33967/facebook-advertising-in-banking/>

¹⁸ <http://www.scribd.com/doc/151089776/FBX-by-the-Numbers-June-2013>;
http://pages.adroll.com/fbx_news_feed_report.html;
<http://www.scribd.com/doc/151089776/FBX-by-the-Numbers-June-2013>

¹⁹ <http://blog.adroll.com/reengage-customers-facebookexchange>

²⁰ <http://www.facebook-pmdcenter.com/profiles/view/11098>

²¹ <http://doublepositiveblogs.com/blog/page/3/>

²² <http://www.facebook-pmdcenter.com/profiles/view/11087>. The only seemingly descriptive words in the profile are “offers user targeting.”

²³ <http://www.appnexus.com>

²⁴ <http://appnexus.com/appnexus-apps>; Compare this with Facebook’s approved description of Appnexus: <http://www.facebook-pmdcenter.com/profiles/view/11087>

²⁵ <http://www.facebook-pmdcenter.com/profiles/view/11099>

recent IPO filing with the SEC, he or she would discover that the company “typically [has] real-time access to the products or services a customer has viewed, researched or bought from them and we continuously receive updated information on approximately 700 million individual products or services, including pricing, images and descriptions.”²⁶ Knowing this, it is apparent that Facebook’s description of this company as “user centric” leaves much to be desired.

The story is the same with other partners as well. One would have to review X+1 documentation to see that it incorporates a wide range of “audience data” for Facebook and related targeting.²⁷

Sharing Covered Information through Cookie-connected Data

In addition to being largely opaque to the average user, these partnerships connect covered information with users’ input into search engines all over the Internet. Facebook has added a user’s search history into its Exchange through its relationship with Chango, which “maintains user profiles linked to search activity on approximately 300 million people in North America” and brings “search intent” data to Facebook from Google and Bing, among others.²⁸ In another example of Facebook’s failure to explain how user data are used for tracking and targeting, one would have to review Facebook Exchange materials on Chango’s website to learn what privacy users lose in this deal. Cookie-connected data are “collected about each individual prior to their arrival on Facebook ... ,” and then used to link advertisers and their targets.²⁹ Facebook Exchange enables a cookie-end user to be targeted on its platform and also pursued via retargeting. (Although Chango, like others, claims the user cookie data are “anonymous,” the Commission increasingly recognizes that such software identifies an individual user).³⁰ Facebook partner Chango describes for clients—not Facebook users—how Programmatic Site Retargeting (PSR) strategies involving Facebook Exchange works: “PSR incorporates visitor behavior from a wide range of sources, including customer profiles, shipping addresses, items in cart. ... [A] cloud-based user profile [is assigned] to each visitor. These profiles allow marketers to gather data on an anonymous user in real time. ... [W]e make this data actionable by giving a ‘visitor score’ to each of the cloud-based profiles”³¹ It is questionable what “anonymous” could mean in a situation where the

²⁶ <http://www.sec.gov/Archives/edgar/data/1576427/000119312513369592/d541385df1.htm>

²⁷ <http://www.xplusone.net/products/origin-data-management-platform>

²⁸ <http://www.adexchanger.com/social-media/facebook-exchange-adds-search-intent-data-as-chango-joins-partner-list/>

²⁹ http://resources.chango.com/rs/changoinc/images/Chango_FBX_Whitepaper.pdf

³⁰ <http://www.ftc.gov/opa/2013/07/coppa.shtm>;
<http://www.ftc.gov/os/caselist/1023185/index.shtm>

³¹ “The Facebook Exchange Handbook.” Available via: <http://www.facebook-pmdecenter.com/profiles/view/11127>; <http://www.adexchanger.com/social-media/facebook-exchange-adds-search-intent-data-as-chango-joins-partner-list/>; <http://www.facebook-pmdecenter.com/profiles/view/11127>; Facebook also enables “realtime dynamic ad creative” changes that takes advantage of the data to further influence users. Given that “Upon receiving a

company claims to have that much information on a user as it follows that user through Facebook. Even if the company acts as if this user's profile is their proprietary data and doesn't regularly share it, the provision of covered information to advertisers is what Facebook said it would not allow, and yet it seems to be Chango's business model.

Sharing User Information through Email Address Matching

Facebook's proposed Data Use policy is designed to enable its recent expanded use of email addresses for targeting users. Facebook relies on email addresses as a key part of its data retargeting in its Facebook Exchange and Partner Categories products.³² Facebook claims that it has an anonymous method of "hashing" email addresses and only giving advertisers a user's information for linking if that anonymous system produces a match. However, Facebook matches users to a much broader data set in many instances, as Facebook notes to developers: "Custom audiences allow advertisers to target their Sponsored Story or ad to *a specific set of users* with whom they have already established a relationship on/off Facebook. Audiences can be defined by either user email address, Facebook UIDs, user phone numbers, app user IDs, or Apple's IDFA."³³ There is nothing anonymous about this method of identifying Facebook users, and linking covered information to these outside data sets makes Facebook liable for all of this information sharing, as the definition of "covered information" includes "any information combined with" any covered information in a user profile.

Facebook explains to marketers this more candid view of Custom Audiences than it does to users:

Custom audiences let marketers find their offline audiences among Facebook users. Using email addresses, phone numbers, Facebook user IDs or app user ID's to make the match, you can now find the exact people you want to talk to, in custom audiences that are defined by what you already know.

This means that in addition to targeting the types of people you want to reach among the Facebook population, you can now also reach segments of specific people based on information you have about your own, offline audiences.

bid request, the advertiser must reply within 120 ms," the speed of the process and its implications for Facebook user privacy should be addressed in its Data policy.
https://developers.facebook.com/docs/reference/ads-api/rtb/#cookie_matching;
<https://www.facebook.com/notes/facebook-and-privacy/relevant-ads-that-protect-your-privacy/457827624267125>; <https://www.facebook.com/about/privacy/other>

³² <https://developers.facebook.com/docs/reference/ads-api/rtb/>;
<http://techcrunch.com/2012/06/13/facebook-exchange/>;
<https://developers.facebook.com/docs/reference/ads-api/partnercategories/>

³³ <https://developers.facebook.com/docs/reference/ads-api/custom-audience-targeting>

You can create a custom audience representing any group of customers or prospect list that you'd like to reach with targeted Facebook Ads. For example, you could run a campaign to get more likes for your Page, targeted at your current customers who have not yet liked your Page.³⁴

Facebook also explains how marketers can use Custom Audiences to find users:

First, identify the groups of customers you'd like to talk to within your contact management system. This might be subsets of current customers, prospects, loyalty club members, current or lapsed users—anyone you want to reach with highly targeted messages.

Then use power editor to find these people on Facebook. Input an email or phone list representing your segments into the power editor. The list will be hashed before being sent to Facebook. The system will match the encrypted data against Facebook's active users, and build a custom audience in your account with everyone that matches your list.³⁵

Facebook claims it doesn't share user data with third parties, but it invites those third parties to provide it with a great amount of user data, so Facebook can target specific users; it also sets the stage for the third party to likely learn that person's identity via retargeting.

Sharing User information through App User IDs

Facebook also fails to explain to users how its new mobile device-targeting service for Custom Audiences works. In May 2013, Facebook

released a new custom audience solution designed specifically for mobile app developers: app user IDs App user IDs extend the benefits of custom audience targeting to mobile in order to solve some of the unique challenges marketers face when remarketing and reengaging their app user bases Adding app user IDs as an additional targeting field for custom audiences solves this challenge, allowing developers to request an encrypted ID from Facebook when someone uses their app.

App developers can now reach and reengage their current user base even if they have not registered with the mobile app upon installing it. For example, a retailer can reach and reengage a person on Facebook who installed their mobile app and browsed particular products, but who may not have necessarily registered their email address or phone number with the retailer

³⁴ <https://www.facebook.com/help/341425252616329>

³⁵ <https://www.facebook.com/help/491619737533280>

Not only can companies with mobile apps now remarket to their user bases with a laser focus with app user IDs, they can do so across devices Thanks to custom audience targeting with app user IDs, marketers can now effectively connect their remarketing and reengagement efforts on mobile to desktop.³⁶

Facebook explains this process in the following manner: “When someone uses your app, you can make a request to Facebook’s servers to request an ID be generated Facebook will return an encrypted ID for that person. (It can also return nothing depending on a person’s choice ...). ... You then send that ID to your server in order to use it later for custom targeting Each call to Facebook’s server to generate an app user ID will *generate a different ID*. Although multiple calls will end up targeting the same person.”³⁷ Once again, Facebook hides behind misleading rhetoric that “no personal customer information (such as demographic, Facebook ID, etc.) is shared with you or advertisers”³⁸ The reality is that the advertiser/developer has shared user information with Facebook, may be able to then use the process to gather PII or related data, and that the social network has gathered additional information about its users. Facebook’s claim that it doesn’t share user information with third parties is both technically incorrect and perverse.

The social network has created a system where it is given abundant personal and data-related information on individual users, is freely able to merge it with its own data, and then has a more robust—and likely ongoing—ability to track and further gather and use their information. Facebook also supplies third parties with user information that they can use to identify specific Facebook users and their activities across devices and platforms. All of this is done without the meaningful ability of a user either to understand or to control how the system operates.

Facebook and App Data

In its proposed Data Use Policy, Facebook adds the phrases “use or are running” and “or about” Facebook, additions that reflect its recent mobile application (“app”) data practice changes, which are now Facebook’s focus in future app development.³⁹ This Last Fall Facebook opened up its “mobile app install ads” to all developers, which are targeted ads designed to trigger users to download apps from developers.⁴⁰ Facebook urged developers to “hyper-target” the app-install ads, which can use email, phone number, and

³⁶ <http://www.nanigans.com/2013/05/21/mobile-ad-targeting-facebook-custom-audiences-app-user-ids/>

³⁷ <https://developers.facebook.com/docs/ads-for-apps/custom-audiences-for-mobile-apps/>

³⁸ <https://developers.facebook.com/docs/ads-for-apps/custom-audiences-for-mobile-apps/>

³⁹ https://lbedn-dragon-a.akamaihd.net/hphotos-ak-prn1/851585_445264755581605_1677569786_n.pdf

⁴⁰ <https://developers.facebook.com/blog/post/2012/10/17/drive-installs-and-discovery-with-mobile-app-install-ads/>

Facebook User ID's as well.⁴¹ Hence developers are using covered information expressly for advertisement targeting, contrary to any statements that such information remains hidden from advertisers.

Facebook has expanded the tracking of users through more than a dozen "mobile measurement" data partners.⁴² For example, its users are unaware what partner Kontagent does and what the partnership between these companies may mean for user privacy and consumer protection. In announcing the relationship, Kontagent explained that "customers who purchase the new mobile app install ad unit on Facebook will, through our Mobile Marketing Analytics, be able to gain deeper insights into levels of user, including engagement, retention, and monetization Kontagent *kSuite DataMine*TM users will be able to analyze the behavior of customers from this new channel down to the most granular level possible."⁴³ The "data insights" Kontagent provides are for companies specializing in, among other things, financial services.⁴⁴ The FTC will have to look at this "most granular" service that tracks individuals' behavior, and see to what extent Facebook users are being made identifiable by these partnerships. The privacy implications of such close tracking must be explored. The Commission should also note reports that "Facebook's mobile app install ad unit is performing well for Financial Services."⁴⁵

Facebook mobile measurement partner Kochava uses device fingerprinting to help "track even the untrackable," something also not told to Facebook users at any point.⁴⁶ It explains that "[b]y using a variety of algorithms which incorporate geo-location, carrier information as well as device information, we can match clicks to installs with an ~85% accuracy rate." The company uses a broad range of identifiers to help it track users across platforms and services.⁴⁷ The use of such techniques that enable the identification of users regardless of where they are online, including mobile phones or PCs, and their connection to Facebook mobile and geo-locational practices raise questions about the efficacy of the consent degree to address contemporary practices. Thus the Commission must review the data collection practices of the mobile measurement partners in light of

⁴¹ <http://www.ampush.com/the-facebook-mobile-app-install-ad-checklist/>; https://fbcdn-dragon-a.akamaihd.net/hphotos-ak-prn1/851563_128604107334977_1765173912_n.pdf

⁴² <https://developers.facebook.com/preferrdmarketingdevelopers/mobile/measurement/>

⁴³ <http://www.kontagent.com/kaleidoscope/2012/11/14/kontagent-facebook-enable-mobile-marketers-to-run-more-effective-campaigns/>

⁴⁴

<https://developers.facebook.com/preferrdmarketingdevelopers/mobile/measurement/#kontagent>

⁴⁵ <http://www.facebook-download.com/uk/2013/03/mobile-success/>

⁴⁶ <https://developers.facebook.com/preferrdmarketingdevelopers/mobile/measurement/#kochava>; <https://kochava.com>. See also, e.g., <https://www.facebook.com/help/www/248716141830800?rdrhc>; <https://www.facebook.com/help/218345114850283>.

⁴⁷ <http://support.kochava.com/customer/portal/articles/960425-server-to-server-integration>; <http://www.mobyaaffiliates.com/mobile-app-marketing/kochava/>

what Facebook’s consent decree commitment, including its privacy-related controls for mobile apps.

In another mobile-related privacy development, Facebook announced to developers on 18 September 2013 that “[i]n addition to using, in a privacy safe way, current customers’ emails, phone numbers, and Facebook UIDs, you can also upload and target specific types of IDs generated from your mobile app to reach relevant people on Facebook.”⁴⁸ It explained that “you can also reach your mobile customers by leveraging Apple’s standard advertising identifier, iOS IDFAs. For example, you can upload a list of your existing customers’ iOS IDFAs into Power Editor, and reach them with relevant information about your app such as an important update. The ability to upload Mobile Advertiser IDs (iOS IDFAs or App User IDs) is available in Power Editor or via our APIs. Go to our tutorial to learn about all of your options for how you may reach your mobile app users through our custom audiences.”⁴⁹ Considering Facebook’s aforementioned departures from truthful descriptions, it is incumbent upon the FTC to review the use of these identifiers rather than taking the company at its word (i.e., “in a privacy safe way,” which is too vague to provide assurances in any case).

Sharing User Information by Creating New Personally Identifiable IDs

As already described, much of Facebook’s matching practices result in sharing covered information, already existing personally identifiable information, or creating new personally identifiable IDs for unique users. To users, such services as Facebook Exchange are described as totally benign. Facebook, in a September 2012 post about “protect[ing] your privacy,” says that it gives its third-party data providers an “ID number (separate from your Facebook ID) for each visitor’s browser. If someone then visits Facebook and his or her browser has that ID, we notify the service provider, who tells us when a marketer wants to show a particular ad.”⁵⁰ Facebook claims to its users that this system “allows marketers to show you ads relevant to your existing relationship with them—and without them needing to send us any personal information about you.”⁵¹ Facebook’s post provides a link regarding its third-party data providers, but it doesn’t identify them.

In the same post Facebook describes its method of matching email addresses so users can be targeted via its “Custom Audiences” ad product.⁵² It explains that “[t]hese hashes [of

⁴⁸ <http://developers.facebook.com/blog/post/2013/09/18/platform-updates--facebook-ios-sdk-3-8--larger-images-for-link-page-posts--and-custom-audiences-upda/>

⁴⁹ <https://developers.facebook.com/blog/post/2013/09/18/platform-updates--facebook-ios-sdk-3-8--larger-images-for-link-page-posts--and-custom-audiences-upda/>

⁵⁰ <https://www.facebook.com/notes/facebook-and-privacy/relevant-ads-that-protect-your-privacy/457827624267125>

⁵¹ <https://www.facebook.com/notes/facebook-and-privacy/relevant-ads-that-protect-your-privacy/457827624267125>

⁵² <https://www.facebook.com/notes/facebook-and-privacy/relevant-ads-that-protect-your-privacy/457827624267125>

email addresses] are bits of text that uniquely identify a piece of data (such as an email address) but are designed to protect against reverse engineering which would reveal that data. Since Facebook and [a representative online] store use the same method to create each hash, we can compare the store's hashes to hashes of addresses in our records and show the ad to any group of users that match."⁵³ But Facebook tells its Facebook Exchange clients another story—that they can “use online, cookie based user intent data to deliver ads [and] leverage your own consumer intent data.”⁵⁴ Facebook urges marketers to use “their own consumer intent data from across the web.”⁵⁵ Illustrating how Facebook utilizes a range of digital data-related marketing practices that impact a user's privacy without meaningful disclosure, it urges data-focused clients to implement on its Exchange “multi-touch attribution, view-through conversions, global frequency capping, day-parting, ... creative optimization [and] retargeting.”⁵⁶ The use of such digital marketing practices involves a range of data collection practices, and reflects the capabilities of Facebook and its third parties to gather more data and non-transparently influence a user's privacy decision-making.⁵⁷

For Ad Exchange clients, Facebook explains its cookie matching process in the following manner: “FBX partners will HTTP 302 redirect from their pixel on an advertiser's site to Facebook's cookie-matching endpoint FBX Partners should specify two redirect endpoints if they wish to receive matched/unmatched responses. The Facebook cookie sync endpoint will redirect to one of the two endpoints based on the result of the match”⁵⁸ The use of “IP address as string with last byte masked” of users needs to be evaluated to determine whether, in combination with other data, user information is being shared without meaningful consent.⁵⁹ CDD believes that this process may convey or facilitate contact information with the user, and needs to be evaluated—at both the technical and contractual levels—for meaningful anonymity. Facebook also permits

⁵³ <https://www.facebook.com/notes/facebook-and-privacy/relevant-ads-that-protect-your-privacy/457827624267125>

⁵⁴ <https://www.facebook-studio.com/fbassets/resource/66/FacebookExchange20120913>

⁵⁵ <https://www.facebook-studio.com/fbassets/resource/66/FacebookExchange20120913>

⁵⁶ <http://marketingland.com/facebook-ad-exchange-fbx-opens-for-business-with-16-partners-21490>

⁵⁷ See for example, <http://www.facebook-download.com/uk/2013/04/attribution-qubit/>; <http://www.kenshoo.com/quantifying-multi-touch-attribution/>; <http://www.nanigans.com/2013/08/28/facebook-exchange-10-steps-to-boost-conversions/>. The Commission should also assess the data collection being processed on the Facebook platform by attribution companies such as Visual IQ, which explains that it has been “tracking advertising activity on Facebook in any and every way it can be tracked since the social network first offered advertising. Our unique, proprietary, pixel-less tracking system pulls in data from all of our clients' digital marketing tools and all of their data sources—including Facebook.” <http://www.visualiq.com/content/visual-iq-perspective-four-crucial-takeaways-attribution-facebook-roi>; <http://www.visualiq.com/content/viq-video-page>

⁵⁸ <https://developers.facebook.com/docs/reference/ads-api/rtb/>

⁵⁹ <https://developers.facebook.com/docs/reference/ads-api/rtb/>

outside marketers to use view through pixels “to facilitate tracking on third-party analytics systems (and associated features like multi-touch attribution, global frequency capping, etc.) FBX allows partners to render view tags alongside a FBX impression.”⁶⁰ CDD also believes that the use of Facebook and industry-wide tracking analytics may enable user identification and contact.

No Meaningful Opt-Out

One has to be knowledgeable about Facebook’s exchange system, and the role of third-party data companies in particular, in order to address its privacy implications. Users are presented with information that makes it appear simple and transparent. For example, Facebook claims in its 30 September 2012 post that “[w]hen we show an FBX ad on Facebook, it includes an ‘X’ link that lets you provide feedback about ads. We also provide a link that lets you learn more about and choose to opt out of future ads from the service provider responsible for that ad.”⁶¹ But rather than giving meaningful information, this process merely directs users to the companies’ boilerplate statements about opting out and general information-use practices.

When one clicks on the X, as we did for a United Airlines ad that was placed by a company named TURN, one goes to an “opt-Out of Turn Ad Targeting” page that doesn’t provide a Facebook user any relevant information on what’s collected or how. The Facebook-linked opt-out does not inform the user of the data sources, targeting categories (such as finance), subsequent data profile sharing, etc. It is, in essence, a blank screen that fails to provide essential information for the expression of meaningful choice.

Similarly, another Facebook ad connects one to a section on Rocket Fuel’s privacy page, which leads to an opt-out statement and links: “Opting Out: It’s a virtuous cycle we’re happy to be part of, and we hope you’re equally happy with your role in this endeavor. But if you’re not, please click here to opt out of personalized ads based on the Rocket Fuel cookie, or here to opt out of other personalized advertising via the Network Advertising Initiative’s opt-out page. If you opt out, you’ll still see ads from us online, and we’ll still do our best to serve the most relevant ads we can. We just won’t know it’s you, so we won’t be able to apply any of your ad preferences.”⁶² These pages are not meant to inform users, but to convince them that opting out is either futile or unimportant. This does not give users information they can assess and weigh in order to make informed decisions about their online privacy

Can You Protect Your Privacy?

Facebook affirmatively states that users can understand and protect their privacy in this new environment: “As part of working with Facebook, we’ve set up these partnerships in a way that people who use Facebook can understand how this advertising works and have

⁶⁰ <https://developers.facebook.com/docs/reference/ads-api/rth/>

⁶¹ <https://www.facebook.com/notes/facebook-and-privacy/relevant-ads-that-protect-your-privacy/457827624267125>

⁶² <http://rocketfuel.com/privacy-policy>

the ability to control it.”⁶³ Facebook describes the various “comprehensive” controls that are available, such as “inline transparency,” “enhanced disclosures, and “data access tools.”⁶⁴ Facebook’s definition of these terms, and what they really mean, need to be questioned by the FTC. Facebook and its partners fail to provide the promised transparency, “enhanced disclosures” and controls. For example, the Facebook help center page for users listing its third-party partners also claims that users can “[l]earn more about these providers and the choices they offer.”⁶⁵ But as with the Sponsored Stories disclosure in the Statement of Rights and Responsibilities (discussed in the accompanying analysis memorandum), users are given a very limited and largely meaningless view of what is collected and how it may be used.

For example, the link for Turn takes one to an opt-out page, which doesn’t disclose anything about its data-use practices; in other words, there are no “enhanced disclosures.”⁶⁶ On Turn’s page opt-outs are offered for the Digital Advertising Alliance and NAI self-regulatory systems and two undefined links related to Turn (“Opt out of Turn, Opt out of TURN Corporate Marketing”).⁶⁷ A user would not be able to make informed privacy choices in this situation because there is no meaningful explanation of what these different links will do, nor of what information Turn might already have. Nowhere listed on Facebook’s Third Party Service Providers page or the link to Turn’s opt out is how Turn’s major data trading desk partners are working with Facebook. According to AdExchanger.com, these include “Omnicom’s Accuen, Aegis’s Amnet and IPG’s Mediabrands Audience Platform.”⁶⁸ As the Commission knows, these are user-data “trading desks” from some of the largest advertising firms in the world. Similarly, Facebook’s link to data partner Xaxis (WPP) takes one to a privacy policy that says it does not collect PII.⁶⁹ For those knowledgeable about the data business, Xaxis is known as the “World’s Largest Pool of Audience Data,” offering “More Consumer Touchpoints than Any Other in the Industry.”⁷⁰ Xaxis’s use of data enables it to target users “with an unprecedented level of precision across multiple digital platforms.”⁷¹ The disconnect

⁶³ <https://www.facebook.com/notes/facebook-and-privacy/advertising-and-our-third-party-partners/532721576777729>

⁶⁴ <https://www.facebook.com/notes/facebook-and-privacy/advertising-and-our-third-party-partners/532721576777729>

⁶⁵ <https://fb-lt.facebook.com/help/www/133547810119620>

⁶⁶ <http://www.turn.com/privacy/optout>

⁶⁷ <http://www.turn.com/privacy/optout>

⁶⁸ <http://www.adexchanger.com/ad-exchange-news/fbx-ftw-partners-share-results-as-facebook-exchange-exits-beta/>

⁶⁹ <https://fb-lt.facebook.com/help/www/133547810119620>

⁷⁰ <http://www.xaxis.com/page/privacy-policy>

⁷¹ <http://www.xaxis.com/news/view/groupm-launches-xaxis-ad-industrys-most-comprehensive-audience-buying->. In this month’s *MIT Technology Review*, both Xaxis and Turn executives are quoted about how they operate with data. <http://www.technologyreview.com/view/518556/a-clearer-picture-companies-define-how-they-add-value-to-the-ad-tech-space/>

between this business model and the idea that the company avoids identifying individuals is something the FTC should examine to understand how Facebook is allowing tracking by Xaxis.⁷²

Facebook data partner DataXu's link also takes users to a privacy opt-out page, which first says it is a site approved by TRUSTe, encouraging individuals to trust this showing of self-regulation.⁷³ Opt-out information is far below on the page and does not offer enhanced disclosures or other controls that Facebook said would be present.⁷⁴ Despite Facebook's stated commitment to transparency and control, its users concerned about their privacy would have to be experts in digital marketing to know that DataXu tells clients they can "Deploy data on Facebook to deliver highly relevant messages to target audiences."⁷⁵ Nor are everyday Facebook users told, despite Facebook's promise to the FTC to provide genuine privacy settings, that data collected from them by DataXu involve the use of "direct A/B tests to compare our results on DataXu for Facebook Exchange to the results we garner from native Facebook targeting as well."⁷⁶ (Such testing impacts users' privacy choices). Nor are Facebook users informed by the DataXu privacy link that the company's data partners include MasterCard, Bluekai, eXelate, Transunion, Lotame, and others about the privacy implications.⁷⁷ The FTC should look at these revelations in light of the Order to discover if omissions of this information amounts to misleading users about how data are used.

One Facebook partner withholds information from users that it had to give to Members of Congress who were investigating data brokers; this reluctance to provide the same quality of information is significant. Epsilon's link from Facebook goes to a complex and obtuse "Marketing and Consumer Choice" page ("Epsilon provides companies the tools to bring relevant and targeted marketing offers to consumers") that provides insufficient disclosure of its practices and is misleading for being overly vague.⁷⁸ Epsilon doesn't tell Facebook users the categories of data it uses, information that was explained in its letter to Rep. Joe Barton and then-Rep. Ed Markey.⁷⁹ In a 14 August 2012 letter responding to an inquiry related to databroker information collection, Epsilon listed some of the "public

⁷² <http://www.businesswire.com/news/home/20110627005401/en/GroupM-Launches-Xaxis-Ad-Industry's-Comprehensive>

⁷³ <https://fb-lt.facebook.com/help/www/133547810119620>; <http://www.dataxu.com/about-us/privacy/data-collection-platform/>

⁷⁴ <http://www.dataxu.com/about-us/privacy/data-collection-platform>

⁷⁵ <http://www.dataxu.com/facebook-preferred-marketing-developer-dataxu-announces-support-facebook-exchange-campaigns/>

⁷⁶ <http://www.dataxu.com/facebook-preferred-marketing-developer-dataxu-announces-support-facebook-exchange-campaigns/>

⁷⁷ <http://www.dataxu.com/partners/partner>

⁷⁸ <http://www.epsilon.com/consumer-preference-center>

⁷⁹ http://www.epsilon.com/pdf/Epsilon_Congressional_Response_8_14_2012.pdf

and private sources and uses” for its data—something Facebook users aren’t informed.⁸⁰ These sources include data from “federal and state governmental agencies, catalog and retail companies, charities, magazines, retailers, utility companies, marketers, and other information brokers.”⁸¹ It also includes “public property records, telephone directories and certain public information posted to social media sites.”⁸² From this limited disclosure, it can be seen that there is nothing anonymous about the information this company is collecting: these are records tied to names, addresses, and other personal information about people.⁸³ Epsilon also gathers and uses geographic, demographic, financial and interest data, and household purchase information—just a few of the 22 primary categories.⁸⁴ Epsilon admits that it “utilize[s] third parties on behalf of its clients” to collect social media data, including “tweets, posts, comments, likes, shares and recommendations.”⁸⁵ These can include “user IDs, names, ages, genders, hometown location, languages and numbers of social connections.”⁸⁶ Nevertheless, Facebook’s link to Epsilon’s privacy page does not convey the range of data that can be used to target and track users on Facebook and off the site.⁸⁷ For example, Facebook users concerned about their finances would surely want to be informed of, and given appropriate comprehensive controls over, Epsilon’s use of financial data. This is especially a concern in light of the linkage of financial data and Facebook: “Facebook advertisers can target people who currently have an auto loan.”⁸⁸

Finally, Axiom’s link from Facebook goes to a page without clear description of data use or any other company practices, although it does off an opt-out.⁸⁹ Users see this phrase at the top of the page, designed to encourage them to allow continued collection:

Opting out, or choosing to have data about you removed from Axiom’s marketing data products, will reduce the amount of unsolicited telemarketing, direct-mail and/or email offers you receive from companies with whom you have not done business. It may also reduce the relevance of offers you receive from companies with whom you have done business

⁸⁰ http://www.epsilon.com/pdf/Epsilon_Congressional_Response_8_14_2012.pdf at

⁸¹ http://www.epsilon.com/pdf/Epsilon_Congressional_Response_8_14_2012.pdf

⁸² http://www.epsilon.com/pdf/Epsilon_Congressional_Response_8_14_2012.pdf

⁸³ Epsilon told the Congressmen that “due to the confidential nature and proprietary nature of our contracts with our sources, we are unable to provide the exact identities of these sources.”
http://www.epsilon.com/pdf/Epsilon_Congressional_Response_8_14_2012.pdf

⁸⁴ http://www.epsilon.com/pdf/Epsilon_Congressional_Response_8_14_2012.pdf

⁸⁵ http://www.epsilon.com/pdf/Epsilon_Congressional_Response_8_14_2012.pdf

⁸⁶ http://www.epsilon.com/pdf/Epsilon_Congressional_Response_8_14_2012.pdf

⁸⁷ See Epsilon link on <https://fb-lt.facebook.com/help/www/133547810119620>

⁸⁸ http://www.epsilon.com/pdf/Epsilon_Congressional_Response_8_14_2012.pdf;
<http://blog.adespresso.com/facebook-partner-categories-guide/>

⁸⁹ <https://isapps.axiom.com/optout/optout.aspx>

since our clients use these products to better understand what offers may be of interest to you.⁹⁰

From that page, a Facebook user would not know how Axiom's data can be used to target them, let alone the privacy consequences of not opting out. One would have to be an industry insider to understand that "Axiom data allows Facebook advertisers to target ads by:

- **Demographics:** If you choose to target by demographic data from Axiom you will be able to reach people by "Home" which includes if the person is an owner, renter, their length of residents and so on. You can also target by household size (1 to 6 people).
- **Financials:** Targeting your Facebook Ads using Financial data from Axiom allows you to reach bank card users, credit card users and investors. Within the credit card category you can segment your reach by gas/department store/retail store card, premium card, travel/entertainment card and upscale department store. You can also reach people based on their typical spending method (cash or credit).
- **Job Role:** Axiom's categories allow you to target your Facebook ads by job role. There are a variety of different options you can choose from including: admin, white collar, blue collar, education, legal professional, financial professional, military, sales, student and more. This ability to target people based on their job may impact LinkedIn Ads, which have traditionally been where marketers go when they need to run a campaign towards specific job types.
- **Purchase History:** Using Axiom's Purchasing category will allow marketers to target users based on what they are spending money on such as: gas, computer electronics, office supplies, travel services, vehicles and more.⁹¹

Axiom's link from Facebook doesn't explain the data used or their privacy implications—which the company provided in a release for clients announcing the alliance earlier this year: "The Facebook-Axiom partnership represents the combination of the social graph data Facebook advertisers can leverage plus, from Axiom, the interests and behaviors consumers have expressed and demonstrated outside Facebook."⁹²

⁹⁰ <https://isapps.axiom.com/optout/optout.aspx>

⁹¹ <http://blog.adespresso.com/facebook-partner-categories-guide/>

⁹² "Partner Categories Drive Better Results for Facebook Advertisers." Axiom/Facebook 2013. Personal copy available upon request; see also: <http://finance.yahoo.com/news/axiom-facebook-improve-online-advertising-151000872.htm>. Facebook also allows advertisers to use tags for Custom Audiences created by its newly acquired Atlas service, something not disclosed. See <http://www.insidefacebook.com/2013/05/22/facebook-adds-atlas-view-tag-support-for-custom-audiences-and-partner-categories/>. The use of Atlas enables advertisers to gather more data on users: "Universal Action Tags enable Atlas clients to add tracking pixels from ad networks, publishers, or other vendors to Atlas action tags that are already placed on advertiser websites." <http://atlassolutions.com/universal-action-tag>. Facebook COO Sheryl Sandberg explained, "We

This ability to “leverage” social information off of Facebook, which is covered information in the Order, is not disclosed in public documents that users can access. None of the three additional links on the Acxiom opt-out page that are said to provide additional information on its U.S. privacy policy and products work. See [Acxiom's U.S. Products Privacy Policy](#); [Acxiom's Marketing Products](#); [What Consumers Should Know](#). Hence, the user is even deprived of boilerplate that the company once had linked to through its unhelpful opt-out page. This review of Acxiom’s actual data practices against the information provided to users should spur FTC to hold Facebook accountable for giving companies like this access to covered information without clearly explaining this to users. The Commission needs to assess the Acxiom and Facebook data relationship, including recent developments in which the data company is helping expand user profiles beyond cookies to a much more robust data set.⁹³

Network Behavior

Facebook says it now accesses users’ network behavior information, but doesn’t tell users what that means.⁹⁴ It has launched a “new tool designed to help telecommunications companies (carriers and operators) bridge the gap between sales, which occur primarily in stores, and ad impressions delivered on Facebook From this starting point, we can establish test and control groups to determine how and when an ad on Facebook correlates to certain actions, such as a group of people switching to new handsets, tablets or carriers.”⁹⁵ In this program, Facebook “analyzes a users’ [sic] mobile phones and wireless provider to see who switches handsets or carriers after looking at specific carrier-based and mobile handset-based ads.”⁹⁶ This is again tracking users much more closely than the words in the official policy, “network behavior,” might alert them to. The FTC should assess whether such close tracking and reporting back to telecom companies—who have plenty of PII on their users to begin with that could be combined with Facebook’s reports through this tool—goes beyond what Facebook has admitted to in its official policies.

believe the Atlas platform will help us demonstrate even more clearly the connection between ad impressions and purchases.” http://allfacebook.com/atlas-view-tags_b118182. The use of Atlas combined with Facebook enables much more granular tracking of users, through attribution methodologies. <http://atlassolutions.com/community/blogpost/115191/atlas-blog/what-atlas-analytics-can-do-for-facebook-advertisers>; <http://allthingsd.com/20130219/the-reason-facebook-is-buying-atlas/>. The FTC should also review the use of Facebook’s “Viewtags” on privacy: <https://developers.facebook.com/docs/reference/ads-api/adgroup/>

⁹³ <http://www.adexchanger.com/data-exchanges/wpp-plimsoll/#more-61289>

⁹⁴ <https://www.facebook.com/facebookforbusiness/news/outcome-measurement>

⁹⁵ <https://www.facebook.com/facebookforbusiness/news/outcome-measurement>

⁹⁶ <http://www.socialnewsdaily.com/16787/facebook-targets-mobile-service-providers/>

Exposing User Data by Connecting Data: Facebook’s New “Entities Graph” is Significantly Changing Data Use

Facebook is increasingly working to track people in everything they *do*, rather than simply advertising to them based on who they say they *are*. This graph analysis, which uses email addresses to help further verify a user’s identity, is done without the conscious awareness or meaningful consent of users. Users may have some knowledge about how Facebook views what it calls the “social graph,” but its Data Use policy doesn’t make transparent what Facebook explains in a June 2013 engineering note that “one way we map them [users] is by traversing the graph of their friendships.”⁹⁷ Facebook says its social graph now “comprises over 1 billion monthly active users, 600 million of who log in every day.”⁹⁸ But these same people are likely unaware—and have not been meaningfully informed—about the ways Facebook uses related data to identify them through what it calls its “Entity Graph.”⁹⁹ The system is a “gargantuan map of relationships,” explained *Wired*.¹⁰⁰ “It provides a kind of digital signature for each Facebook user and the world he or she inhabits.”¹⁰¹ Facebook’s data system learns about user behavior that is then made actionable, for advertisers and others.¹⁰² As Facebook explained in its June 2013 post:

People don’t just have connections to other people—they may use Facebook to check in to restaurants and other points of interest, they might show their favorite books and movies on their timeline, and they may also list their high school, college and workplace. These 100+ billion connections form the *entity graph*.¹⁰³

Users do not know that Facebook’s data analytics machinery is continually using their information to construct algorithms designed to take advantage of this user-related information, and how they interact in the world (including actions involving the “like” button, check-ins, etc.).¹⁰⁴

⁹⁷ <https://www.facebook.com/notes/facebook-engineering/under-the-hood-the-entities-graph/10151490531588920>

⁹⁸ <https://www.facebook.com/notes/facebook-engineering/under-the-hood-the-entities-graph/10151490531588920>

⁹⁹ See <https://www.facebook.com/notes/facebook-engineering/under-the-hood-the-entities-graph/10151490531588920>

¹⁰⁰ <http://www.wired.com/wiredenterprise/2013/07/entities-graph/>

¹⁰¹ <http://www.wired.com/wiredenterprise/2013/07/entities-graph/>

¹⁰² <http://www.socialnewsdaily.com/16787/facebook-targets-mobile-service-providers>

¹⁰³ <https://www.facebook.com/notes/facebook-engineering/under-the-hood-the-entities-graph/10151490531588920>

¹⁰⁴ <https://www.facebook.com/notes/facebook-engineering/under-the-hood-the-entities-graph/10151490531588920>

Facebook engineers have “loaded millions of entries into the entity graph by simply watching what people do on Facebook. Entities such as colleges and employers are learned from data typed into profile pages; businesses, movies, fictional characters, and other concepts are learned from fan pages created by Facebook users Facebook is now littered with tiny nudges to encourage people to contribute more directly”¹⁰⁵ Facebook’s new graph search product takes advantage of this graph-focused data analysis. Facebook’s graph “includes the relationships between” users, the pages they view, and “other objects within the Facebook universe.”¹⁰⁶ Each “entity, or node within the Facebook graph” is identified by “a unique number called a fbid (Facebook ID) [that] has a set of attributes, or metadata associated with it. The relationships between these nodes, called edges, contain their own metadata to describe the type of relationship between them.”¹⁰⁷ Once everything has a tracking number, everyone can be tracked: “You can learn what entities are close to a certain location, liked by certain people, or otherwise tethered to a user through the social network’s path of edges.”¹⁰⁸ The FTC must look at this increased data availability and determine if it is going to get in the way of user privacy in ways that Facebook does not bring up.

Other

To understand better how Facebook works to advance the data-gathering activities of its major advertisers, the FTC should review The Facebook Studio Gallery, the actual operations of its preferred ad related developers, and other resources.¹⁰⁹

¹⁰⁵ <http://m.technologyreview.com/news/511591/facebook-nudges-users-to-catalog-the-real-world/>

¹⁰⁶ <http://arstechnica.com/information-technology/2013/03/knowning-the-score-how-facebooks-graph-search-knows-what-you-want/>

¹⁰⁷ <http://arstechnica.com/information-technology/2013/03/knowning-the-score-how-facebooks-graph-search-knows-what-you-want/>

¹⁰⁸ <http://arstechnica.com/information-technology/2013/03/knowning-the-score-how-facebooks-graph-search-knows-what-you-want/>

¹⁰⁹ <https://www.facebook-studio.com/gallery/>; <https://www.facebook-studio.com/directory/>; <https://www.facebook-studio.com/education/index>

From: Mithal, Maneesha </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=MMITHAL>
Sent: Thursday, November 7, 2013 6:37 PM
To: Rich, Jessica L. <JRICH@ftc.gov>
Subject: Fw: Cal AG collaboration

(b)(5)

From: Berger, Laura
Sent: Thursday, November 07, 2013 06:34 PM
To: Olsen, Christopher; Mithal, Maneesha
Subject: RE: Cal AG collaboration

(b)(5)

From: Berger, Laura
Sent: Thursday, November 07, 2013 9:22 AM
To: Olsen, Christopher; Mithal, Maneesha
Subject: RE: Cal AG collaboration

(b)(5)

From: Olsen, Christopher
Sent: Wednesday, November 06, 2013 7:01 PM
To: Berger, Laura; Mithal, Maneesha
Subject: Re: Cal AG collaboration

(b)(5)

From: Berger, Laura
Sent: Wednesday, November 06, 2013 07:15 PM
To: Mithal, Maneesha; Olsen, Christopher
Subject: RE: Cal AG collaboration

(b)(5)

From: Rich, Jessica L.
Sent: Wednesday, November 06, 2013 4:10 PM
To: Mithal, Maneesha; Kaufman, Daniel; Berger, Laura; Olsen, Christopher
Subject: Cal AG collaboration

(b)(5)

Jessica L. Rich, Director
Bureau of Consumer Protection
Federal Trade Commission

From: Rich, Jessica L.
Sent: Friday, November 01, 2013 08:32 AM
To: Mithal, Maneesha; Kaufman, Daniel; Berger, Laura
Subject: Fw: touching base

(b)(5)

Jessica L. Rich, Director
Bureau of Consumer Protection

Federal Trade Commission

From: Jeffrey Rabkin [<mailto:Jeffrey.Rabkin@doj.ca.gov>]
Sent: Friday, November 01, 2013 09:29 AM
To: Rich, Jessica L.
Subject: touching base

(b)(5)

— Jeff

Jeffrey Rabkin
Special Assistant Attorney General
Tel: (415) 703-1008

CONFIDENTIALITY NOTICE: This communication with its contents may contain confidential and/or legally privileged information. It is solely for the use of the intended recipient(s). Unauthorized interception, review, use or disclosure is prohibited and may violate applicable laws including the Electronic Communications Privacy Act. If you are not the intended recipient, please contact the sender and destroy all copies of the communication.

From: Mithal, Maneesha </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=MMITHAL>
Sent: Friday, November 8, 2013 6:53 PM
To: Berger, Laura <LBERGER@ftc.gov>; Olsen, Christopher <colsen@ftc.gov>
Subject: Fw: Cal AG collaboration

(b)(5)

From: Rich, Jessica L
Sent: Friday, November 08, 2013 06:52 PM
To: Mithal, Maneesha
Subject: Re: Cal AG collaboration

(b)(5)

Jessica L. Rich, Director
Bureau of Consumer Protection
Federal Trade Commission

Duplicate

From: Olsen, Christopher </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/
CN=RECIPIENTS/CN=COLSEN>
Sent: Wednesday, November 6, 2013 9:34 AM
To: Mithal, Maneesha <MMITHAL@ftc.gov>
Subject: FW: CNOs FB summary for 11.06.13 mtg(ldb eds).docx
Attach: CNOs FB summary for 11.06.13 mtg(ldb eds).docx

(b)(5)

From: Berger, Laura
Sent: Tuesday, November 05, 2013 12:36 PM
To: Olsen, Christopher
Subject: CNOs FB summary for 11.06.13 mtg(ldb eds).docx

From: Mithal, Maneesha </o=FTCEXCHANGE/ou=First Administrative Group/cn=Recipients/cn=MMITHAL>
Sent: Tuesday, November 12, 2013 9:10 AM
To: Berger, Laura <LBERGER@ftc.gov>; Olsen, Christopher <colsen@ftc.gov>
Subject: FW: Facebook Memo
Attach: Memo Attachments.pdf; Commission memo (sent.8nov2013 DRAFT).docx

From: Kohm, James A.
Sent: Friday, November 08, 2013 3:44 PM
To: Rich, Jessica L.; Mithal, Maneesha
Subject: FW: Facebook Memo

From: Koss, Laura
Sent: Friday, November 08, 2013 2:14 PM
To: Kohm, James A.
Cc: Kim, Laura; Kim, Reenah
Subject: Facebook Memo

Enclosed please find our Memorandum to Chairwoman Ramirez on Facebook and the accompanying attachments.

Laura Koss
Senior Attorney
Federal Trade Commission | Division of Enforcement
600 Pennsylvania Ave., N.W. | Mail Drop M-8102B | Washington DC 20580
t: 202.326.2890 | f: 202.326.2558 | lkoss@ftc.gov

**UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION**

COMMISSIONERS: **Jon Leibowitz, Chairman**
 J. Thomas Rosch
 Edith Ramirez
 Julie Brill
 Maureen K. Ohlhausen

In the Matter of)

FACEBOOK, INC.,)
a corporation.)
)

DOCKET NO. C-4365

DECISION AND ORDER

The Federal Trade Commission, having initiated an investigation of certain acts and practices of the Respondent named in the caption hereof, and the Respondent having been furnished thereafter with a copy of a draft Complaint that the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued, would charge the Respondent with violation of the Federal Trade Commission Act, 15 U.S.C. § 45 *et seq.*;

The Respondent and counsel for the Commission having thereafter executed an Agreement Containing Consent Order (“Consent Agreement”), an admission by the Respondent of all the jurisdictional facts set forth in the aforesaid draft Complaint, a statement that the signing of said Consent Agreement is for settlement purposes only and does not constitute an admission by the Respondent that the law has been violated as alleged in such Complaint, or that the facts as alleged in such Complaint, other than jurisdictional facts, are true, and waivers and other provisions as required by the Commission’s Rules; and

The Commission having thereafter considered the matter and having determined that it has reason to believe that the Respondent has violated the Federal Trade Commission Act, and that a Complaint should issue stating its charges in that respect, and having thereupon accepted the executed Consent Agreement and placed such Consent Agreement on the public record for a period of thirty (30) days for the receipt and consideration of public comments, and having carefully considered the comments filed by interested persons, now in further conformity with

the procedure described in Commission Rule 2.34, 16 C.F.R. § 2.34, the Commission hereby issues its Complaint, makes the following jurisdictional findings, and enters the following order:

1. Respondent Facebook, Inc. ("Facebook") is a Delaware corporation with its principal office or place of business at 1601 Willow Road, Menlo Park, California 94025.
2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the Respondent, and the proceeding is in the public interest.

ORDER

DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. Unless otherwise specified, "Respondent" shall mean Facebook, its successors and assigns. For purposes of Parts I, II, and III of this order, "Respondent" shall also mean Facebook acting directly, or through any corporation, subsidiary, division, website, or other device.
2. "Commerce" shall be defined as it is defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.
3. "Clear(ly) and prominent(ly)" shall mean:
 - A. in textual communications (*e.g.*, printed publications or words displayed on the screen of a computer or mobile device), the required disclosures are of a type, size, and location sufficiently noticeable for an ordinary consumer to read and comprehend them, in print that contrasts highly with the background on which they appear;
 - B. in communications disseminated orally or through audible means (*e.g.*, radio or streaming audio), the required disclosures are delivered in a volume and cadence sufficient for an ordinary consumer to hear and comprehend them;
 - C. in communications disseminated through video means (*e.g.*, television or streaming video), the required disclosures are in writing in a form consistent with subpart (A) of this definition and shall appear on the screen for a duration sufficient for an ordinary consumer to read and comprehend them, and in the same language as the predominant language that is used in the communication; and
 - D. in all instances, the required disclosures: (1) are presented in an understandable language and syntax; and (2) include nothing contrary to, inconsistent with, or in

mitigation of any statement contained within the disclosure or within any document linked to or referenced therein.

4. "Covered information" shall mean information from or about an individual consumer including, but not limited to: (a) a first or last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a mobile or other telephone number; (e) photos and videos; (f) Internet Protocol ("IP") address, User ID or other persistent identifier; (g) physical location; or (h) any information combined with any of (a) through (g) above.
5. "Nonpublic user information" shall mean covered information that is restricted by one or more privacy setting(s).
6. "Privacy setting" shall include any control or setting provided by Respondent that allows a user to restrict which individuals or entities can access or view covered information.
7. "Representatives" shall mean Respondent's officers, agents, servants, employees, attorneys, and those persons in active concert or participation with them who receive actual notice of this Order by personal service or otherwise.
8. "Third party" shall mean any individual or entity that uses or receives covered information obtained by or on behalf of Respondent, other than: (1) a service provider of Respondent that (i) uses the covered information for and at the direction of Respondent and no other individual or entity and for no other purpose; and (ii) does not disclose the covered information, or any individually identifiable information derived from such covered information, except for, and at the direction of, Respondent, for the purpose of providing services requested by a user and for no other purpose; or (2) any entity that uses the covered information only as reasonably necessary: (i) to comply with applicable law, regulation, or legal process, (ii) to enforce Respondent's terms of use, or (iii) to detect, prevent, or mitigate fraud or security vulnerabilities.
9. "User" shall mean an identified individual from whom Respondent has obtained information for the purpose of providing access to Respondent's products and services.

I.

IT IS ORDERED that Respondent and its representatives, in connection with any product or service, in or affecting commerce, shall not misrepresent in any manner, expressly or by implication, the extent to which it maintains the privacy or security of covered information, including, but not limited to:

- A. its collection or disclosure of any covered information;

- B. the extent to which a consumer can control the privacy of any covered information maintained by Respondent and the steps a consumer must take to implement such controls;
- C. the extent to which Respondent makes or has made covered information accessible to third parties;
- D. the steps Respondent takes or has taken to verify the privacy or security protections that any third party provides;
- E. the extent to which Respondent makes or has made covered information accessible to any third party following deletion or termination of a user's account with Respondent or during such time as a user's account is deactivated or suspended; and
- F. the extent to which Respondent is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy, security, or any other compliance program sponsored by the government or any third party, including, but not limited to, the U.S.-EU Safe Harbor Framework.

II.

IT IS FURTHER ORDERED that Respondent and its representatives, in connection with any product or service, in or affecting commerce, prior to any sharing of a user's nonpublic user information by Respondent with any third party, which materially exceeds the restrictions imposed by a user's privacy setting(s), shall:

- A. clearly and prominently disclose to the user, separate and apart from any "privacy policy," "data use policy," "statement of rights and responsibilities" page, or other similar document: (1) the categories of nonpublic user information that will be disclosed to such third parties, (2) the identity or specific categories of such third parties, and (3) that such sharing exceeds the restrictions imposed by the privacy setting(s) in effect for the user; and
- B. obtain the user's affirmative express consent.

Nothing in Part II will (1) limit the applicability of Part I of this order; or (2) require Respondent to obtain affirmative express consent for sharing of a user's nonpublic user information initiated by another user authorized to access such information, provided that such sharing does not materially exceed the restrictions imposed by a user's privacy setting(s). Respondent may seek modification of this Part pursuant to 15 U.S.C. §45(b) and 16 C.F.R. 2.51(b) to address relevant developments that affect compliance with this Part, including, but not limited to, technological changes and changes in methods of obtaining affirmative express consent.

III.

IT IS FURTHER ORDERED that Respondent and its representatives, in connection with any product or service, in or affecting commerce, shall, no later than sixty (60) days after the date of service of this order, implement procedures reasonably designed to ensure that covered information cannot be accessed by any third party from servers under Respondent's control after a reasonable period of time, not to exceed thirty (30) days, from the time that the user has deleted such information or deleted or terminated his or her account, except as required by law or where necessary to protect the Facebook website or its users from fraud or illegal activity. Nothing in this paragraph shall be construed to require Respondent to restrict access to any copy of a user's covered information that has been posted to Respondent's websites or services by a user other than the user who deleted such information or deleted or terminated such account.

IV.

IT IS FURTHER ORDERED that Respondent shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive privacy program that is reasonably designed to (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information. Such program, the content and implementation of which must be documented in writing, shall contain controls and procedures appropriate to Respondent's size and complexity, the nature and scope of Respondent's activities, and the sensitivity of the covered information, including:

- A. the designation of an employee or employees to coordinate and be responsible for the privacy program.
- B. the identification of reasonably foreseeable, material risks, both internal and external, that could result in Respondent's unauthorized collection, use, or disclosure of covered information and an assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this privacy risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management, including training on the requirements of this order, and (2) product design, development, and research.
- C. the design and implementation of reasonable controls and procedures to address the risks identified through the privacy risk assessment, and regular testing or monitoring of the effectiveness of those controls and procedures.
- D. the development and use of reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from Respondent and requiring service providers, by contract, to

implement and maintain appropriate privacy protections for such covered information.

- E. the evaluation and adjustment of Respondent's privacy program in light of the results of the testing and monitoring required by subpart C, any material changes to Respondent's operations or business arrangements, or any other circumstances that Respondent knows or has reason to know may have a material impact on the effectiveness of its privacy program.

V.

IT IS FURTHER ORDERED that, in connection with its compliance with Part IV of this order, Respondent shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. A person qualified to prepare such Assessments shall have a minimum of three (3) years of experience in the field of privacy and data protection. All persons selected to conduct such Assessments and prepare such reports shall be approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, in his or her sole discretion. Any decision not to approve a person selected to conduct such Assessments shall be accompanied by a writing setting forth in detail the reasons for denying such approval. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

- A. set forth the specific privacy controls that Respondent has implemented and maintained during the reporting period;
- B. explain how such privacy controls are appropriate to Respondent's size and complexity, the nature and scope of Respondent's activities, and the sensitivity of the covered information;
- C. explain how the privacy controls that have been implemented meet or exceed the protections required by Part IV of this order; and
- D. certify that the privacy controls are operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by Respondent until the order is

terminated and provided to the Associate Director of Enforcement within ten (10) days of request.

VI.

IT IS FURTHER ORDERED that Respondent shall maintain and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of:

- A. for a period of three (3) years from the date of preparation or dissemination, whichever is later, all widely disseminated statements by Respondent or its representatives that describe the extent to which Respondent maintains and protects the privacy, security, and confidentiality of any covered information, including, but not limited to, any statement related to a change in any website or service controlled by Respondent that relates to the privacy of such information, along with all materials relied upon in making such statements, and a copy of each materially different privacy setting made available to users;
- B. for a period of six (6) months from the date received, all consumer complaints directed at Respondent or forwarded to Respondent by a third party, that relate to the conduct prohibited by this order and any responses to such complaints;
- C. for a period of five (5) years from the date received, any documents, prepared by or on behalf of Respondent, that contradict, qualify, or call into question Respondent's compliance with this order;
- D. for a period of three (3) years from the date of preparation or dissemination, whichever is later, each materially different document relating to Respondent's attempt to obtain the consent of users referred to in Part II above, along with documents and information sufficient to show each user's consent; and documents sufficient to demonstrate, on an aggregate basis, the number of users for whom each such privacy setting was in effect at any time Respondent has attempted to obtain and/or been required to obtain such consent; and
- E. for a period of three (3) years after the date of preparation of each Assessment required under Part V of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of Respondent, including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, for the compliance period covered by such Assessment.

VII.

IT IS FURTHER ORDERED that Respondent shall deliver a copy of this order to (1) all current and future principals, officers, directors, and managers; (2) all current and future employees, agents, and representatives having supervisory responsibilities relating to the subject matter of this order, and (3) any business entity resulting from any change in structure set forth in Part VIII. Respondent shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities. For any business entity resulting from any change in structure set forth in Part VIII, delivery shall be at least ten (10) days prior to the change in structure.

VIII.

IT IS FURTHER ORDERED that Respondent shall notify the Commission within fourteen (14) days of any change in Respondent that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in either corporate name or address. Unless otherwise directed by a representative of the Commission, all notices required by this Part shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the Matter of Facebook, Inc.*, FTC File No.[]. *Provided, however*, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.

IX.

IT IS FURTHER ORDERED that Respondent, within ninety (90) days after the date of service of this order, shall file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of their own compliance with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, Respondent shall submit additional true and accurate written reports.

X.

This order will terminate on July 27, 2032, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

- A. any Part of this order that terminates in fewer than twenty (20) years; and
- B. this order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that Respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Part as though the complaint had never been filed, except that this order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission, Commissioner Rosch dissenting and Commissioner Ohlhausen not participating.

Donald S. Clark
Secretary

SEAL
ISSUED: July 27, 2012

Data Use Policy

Date of Last Revision: ~~December 11, 2012~~ September ##, 2013

I. Information we receive and how it is used

Information we receive about you

We receive a number of different types of information about you, including:

Your information

Your information is the information that's required when you sign up for the site, as well as the information you choose to share.

- **Registration information:** When you sign up for Facebook, you are required to provide information such as your name, email address, birthday, and gender. In some cases, you may be able to register using other information, like your telephone number.
- **Information you choose to share:** Your information also includes the information you choose to share on Facebook, such as when you post a status update, upload a photo, or comment on a friend's story.

It also includes the information you choose to share when you communicate with us, such as when you contact us using an email address, or when you take an action, such as when you add a friend, like a Page or a website, add a place to your story, use our contact importers, or indicate you are in a relationship.

☞ Your name, profile pictures, cover photos, gender, networks, username and User ID are treated just like information you choose to make public.

☞ Your birthday allows us to do things like show you age-appropriate content and advertisements.

Information others share about you

We receive information about you from your friends and others, such as when they upload your contact information, post a photo of you, tag you in a photo or status update, or at a location, or add you to a group.

☞ When people use Facebook, they may store and share information about you and others that they have, such as when they upload and manage their invites and contacts.

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 ~~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.
- When you post things like photos or videos on Facebook, we may receive additional related data (or metadata), such as the time, date, and place you took the photo or video.
- We receive data from or about the computer, mobile phone, or other devices you use to install Facebook apps or to access Facebook, including when multiple users log in from the same device. This may include network and communication information, such as your IP address or mobile phone number, and other information about things like your internet service, operating system, location, the type (including identifiers) of the device or browser you use, or the pages you visit. For example, we may get your GPS or other location information so we can tell you if any of your friends are nearby, or we could request device information to improve how our apps work on your device.
- We receive data whenever you visit a game, application, or website that uses Facebook Platform or visit a site with a Facebook feature (such as a social plugin), sometimes through cookies. This may include the date and time you visit the site; the web address, or URL, you're on; technical information about the IP address, browser and the operating system you use; and, if you are logged in to Facebook, your User ID.
- Sometimes we get data from our affiliates or our advertising partners, customers and other third parties that helps us (or them) deliver ads, understand online activity, and generally make Facebook better. For example, an advertiser may tell us information about you (like how you responded to an ad on Facebook or on another site) in order to measure the effectiveness of - and improve the quality of - ads.

As described in "How we use the information we receive," ~~We-we~~ we also put together data from the information we already have about you, and your friends, and others, so we can offer and suggest a variety of services and features. For example, we may ~~put together data about you to determine-make~~ make friend suggestions, pick stories which for friends we should show you in your News Feed, or suggest people you to tag in the photos you post. We may put together your current city with GPS and other location information we have about you to, for example, tell you and your friends about people or events nearby, or offer deals to you in which that you might be interested in. We may also put together data about you to serve you ads or other content that might be more relevant to you.

☞ When we get your GPS location, we put it together with other location information we have about you (like your current city). But we only keep it until it is no longer useful to provide you services, like keeping your last GPS coordinates to send you relevant notifications.

☞ We only provide data to our advertising partners or customers after we have removed your name or any other personally identifying information from it, or have combined it with other people's data in a way that it ~~is no longer~~ personally identifies ~~associated with~~ you.

Public information

When we use the phrase "public information" (which we sometimes refer to as "Everyone information"), we mean the information you choose to make public, as well as information that is always publicly available.

Information you choose to make public

Choosing to make your information public is exactly what it sounds like: **anyone**, including people off of Facebook, will be able to see it.

Choosing to make your information public also means that this information:

- can be associated with you (i.e., your name, profile pictures, cover photos, timeline, User ID, username, etc.) even off Facebook;
- can show up when someone does a search on Facebook or on a public search engine;
- will be accessible to the Facebook-integrated games, applications, and websites you and your friends use; and
- will be accessible to anyone who uses our APIs such as our [Graph API](#).

☞ Sometimes you will not be able to select an audience when you post something (like when you write on a Page's wall or comment on a news article that uses our comments plugin). This is because some types of stories are always public stories. As a general rule, you should assume that if you do not see a [sharing icon](#), the information will be publicly available.

☞ When others share information about you, they can also choose to make it public.

Information that is always publicly available

The types of information listed below are always publicly available, and they are treated just like information you decided to make public:

- **Name:** This helps your friends and family find you. If you are uncomfortable sharing your real name, you can always [delete](#) your account.
- **Profile Pictures and Cover Photos:** These help your friends and family recognize you. If you are uncomfortable making any of these photos public, you can always [delete them](#). Unless you delete them, when you add a new profile picture or cover photo, the previous photo will remain public in your profile picture or cover photo album.
- **Networks:** This helps you see whom you will be sharing information with before you choose "Friends and Networks" as a custom audience. If you are uncomfortable making your network public, you can [leave the network](#).
- **Gender:** This allows us to refer to you properly.

- **Username and User ID:** These allow you to give out a custom link to your timeline or Page, receive email at your Facebook email address, and help make Facebook Platform possible.

Usernames and User IDs

~~Usernames and User IDs are the same thing – a way to identify you on Facebook. A User ID is a string of numbers and a username generally is some variation of your name. With your username, you get a custom link (a Facebook URL, such as www.facebook.com/username) to your timeline that you can give out to people or post on external websites. Usernames appear in the URL on your timeline. We also use your User ID to identify your Facebook account.~~

If someone has your Username or User ID, they can use it to access information about you through the facebook.com website. For example, if someone has your Username, they can type facebook.com/Username into their browser and see your public information as well as anything else you've let them see. Similarly, someone with your Username or User ID can access information about you through our APIs, such as our [Graph API](#). Specifically, they can access your public information, along with your age range, language and country.

If you do not want your information to be accessible to Platform applications, you can turn off all Platform applications from your Privacy Settings. If you turn off Platform you will no longer be able to use any games or other applications until you turn Platform back on. For more information about the information that apps receive when you visit them, see [Other websites and applications](#).

☞ If you want to see information available about you through our Graph API, just type [https://graph.facebook.com/\[User ID or Username\]?metadata=1](https://graph.facebook.com/[User ID or Username]?metadata=1) into your browser.

☞ Your Facebook email address includes your public username like so: username@facebook.com. ~~People can use your Facebook email address to send you messages and Anyone in a message conversation can reply to it.~~

How we use the information we receive

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

- as part of our efforts to keep Facebook products, services and integrations safe and secure;
- to protect Facebook's or others' rights or property;
- to provide you with location features and services, like telling you and your friends when something is going on nearby;

- to measure or understand the effectiveness of ads you and others see, including to deliver relevant ads to you;
- to make suggestions to you and other users on Facebook, such as: suggesting that your friend use our contact importer because you found friends using it, suggesting that another user add you as a friend because the user imported the same email address as you did, or suggesting that your friend tag you in a picture they have uploaded with you in it; and
- for internal operations, including troubleshooting, data analysis, testing, research and service improvement.

Granting us ~~this~~ permission to use your information not only allows us to provide Facebook as it exists today, but it also allows us to provide you with innovative features and services we develop in the future that use the information we receive about you in new ways.

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

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

Of course, for information others share about you, they control how it is shared.

We store data for as long as it is necessary to provide products and services to you and others, including those described above. Typically, information associated with your account will be kept until your account is deleted. For certain categories of data, we may also tell you about specific data retention practices.

⚠ We may enable access to public information that has been shared through our services, or allow service providers to access information so they can help us provide services.

⚠ We are able to suggest that your friend tag you in a picture by scanning and comparing your friend's pictures to information we've put together from your profile pictures and the other photos in which you've been tagged. ~~in. This allows us to make these suggestions.~~ You can control whether we suggest that another user tag you in a photo using the "How Tags work Timeline and Tagging" settings. Learn more at: <https://www.facebook.com/help/tag-suggestions>

Deleting and deactivating your account

If you want to stop using your account, you can either **deactivate** or **delete** it.

Deactivate

Deactivating your account puts your account on hold. Other users will no longer see your timeline, but we do not delete any of your information. Deactivating an account is the same as

you telling us not to delete any information because you might want to reactivate your account at some point in the future. You can deactivate your account at:

<https://www.facebook.com/settings?tab=security>

☞ Your friends will still see you listed in their list of friends while your account is deactivated.

Deletion

When you delete your ~~own~~ account, it is permanently deleted from Facebook. It typically takes about one month to delete an account, but some information may remain in backup copies and logs for up to 90 days. You should only delete your account if you are sure you never want to reactivate it. You can delete your account at:

https://www.facebook.com/help/contact.php?show_form=delete_account

Learn more at: <https://www.facebook.com/help/?faq=356107851084108>

☞ Certain information is needed to provide you with services, so we only delete this information after you delete your account. Some of the things you do on Facebook aren't stored in your account, like posting to a group or sending someone a message (where your friend may still have a message you sent, even after you delete your account). That information remains after you delete your account.

II. Sharing and finding you on Facebook

Control each time you post

Whenever you post content (like a status update, photo or check-in), you can select a specific audience, or even customize your audience. To do this, simply click on the sharing icon and choose who can see it.

☞ Choose this icon if you want to make something **Public**. Choosing to make something public is exactly what it sounds like. It means that anyone, including people off of Facebook, will be able to see or access it.

☞ Choose this icon if you want to share with your Facebook **Friends**.

☞ Choose this icon if you want to **Customize** your audience. You can also use this to hide your story from specific people.

If you tag someone, that person and their friends can see your story no matter what audience you selected. The same is true when you approve a tag someone else adds to your story.

Always think before you post. Just like anything else you post on the web or send in an email, information you share on Facebook can be copied or re-shared by anyone who can see it.

☞ Although you choose with whom you share, there may be ways for others to determine information about you. For example, if you hide your birthday so no one can see it on your timeline, but friends post "happy birthday!" on your timeline, people may determine your birthday.

☞ When you comment on or "like" someone else's story, or write on their timeline, that person gets to select the audience. For example, if a friend posts a Public story and you comment on it,

your comment will be Public. Often, you can see the audience someone selected for their story before you post a comment; however, the person who posted the story may later change their audience. So, if you comment on a story, and the story's audience changes, the new audience can see your comment.

☞ You can control who can see the Facebook Pages you've "liked" by visiting your timeline, clicking on the Likes box on your timeline, and then clicking "Edit."

☞ Sometimes you will not see a sharing icon when you post something (like when you write on a Page's wall or comment on a news article that uses our comments plugin). This is because some types of stories are always public stories. As a general rule, you should assume that if you do not see a sharing icon, the information will be publicly available.

Control over your timeline

Whenever you add things to your timeline you can select a specific audience, or even customize your audience. To do this, simply click on the sharing icon and choose who can see it.

☞ Choose this icon if you want to make something **Public**. Choosing to make something public is exactly what it sounds like. It means that anyone, including people off of Facebook, will be able to see or access it.

☞ Choose this icon if you want to share with your Facebook **Friends**.

☞ Choose this icon if you want to **Customize** your audience. You can also use this to hide the item on your timeline from specific people.

When you select an audience for your friend list, you are only controlling who can see the entire list of your friends on your timeline. We call this a timeline visibility control. This is because your friend list is always available to the games, applications and websites you use, and your friendships may be visible elsewhere (such as on your friends' timelines or in searches). For example, if you select "Only Me" as the audience for your friend list, but your friend sets her friend list to "Public," anyone will be able to see your connection on your friend's timeline. Similarly, if you choose to hide your gender, it only hides it on your timeline. This is because we, just like the applications you and your friends use, need to use your gender to refer to you properly on the site.

When someone tags you in a story (such as a photo, status update or check-in), you can choose whether you want that story to appear on your timeline. You can either approve each story individually or approve all stories by your friends. If you approve a story and later change your mind, you can remove it from your timeline.

☞ When you hide things on your timeline, like posts or connections, it means those things will not appear on your timeline. But, remember, anyone in the audience of those posts or who can see a connection may still see it elsewhere, like on someone else's timeline or in search results. You can also delete your posts or change the audience of content you post, which means you can remove people from or add people to the audience of the content.

☞ People on Facebook may be able to see mutual friends, even if they cannot see your entire list of friends.

☞ Some things (like your name, profile pictures and cover photos) do not have sharing icons because they are always publicly available. As a general rule, you should assume that if you do not see a sharing icon, the information will be publicly available.

Finding you on Facebook

To make it easier for your friends to find you, we allow anyone with your contact information (such as email address or telephone number) to find you through the Facebook search bar at the top of most pages, as well as other tools we provide, such as contact importers - even if you have not shared your contact information with them on Facebook.

You can choose who can look up your timeline using the email address or telephone number you added to your timeline through your [Privacy Settings](#). But remember that people can still find you or a link to your timeline on Facebook through other people and the things they share about you or through other posts, like if you are tagged in a friend's photo or post something to a public page.

☞ Your settings do not control whether people can find you or a link to your timeline when they search for content they have permission to see, like a photo or other story in which you've been tagged in.

Access on phones and other devices

Once you share information with your friends and others, they may be able to sync it with or access it via their mobile phones and other devices. For example, if you share a photo on Facebook, someone viewing that photo could save it using Facebook tools or by other methods offered by their device or browser. Similarly, if you share your contact information with someone or invite someone to an event, they may be able to use Facebook or third party applications or devices to sync that information. Or, if one of your friends has a Facebook application on one of their devices, your information (such as the things you post or photos you share) may be stored on or accessed by their device.

☞ You should only share information with people you trust because they will be able to save it or re-share it with others, including when they sync the information to a device.

Activity log

Your activity log is a place where you can go to view most of your information on Facebook, including things you've hidden from your timeline. You can use this log to manage your content. For example, you can do things like delete stories, change the audience of your stories or stop an application from publishing to your timeline on your behalf.

☞ When you hide something from your timeline, you are not deleting it. This means that the story may be visible elsewhere, like in your friends' News Feed. If you want to delete a story you posted, choose the delete option.

What your friends and others share about you

Links and Tags

Anyone can add a link to a story. Links are references to something on the Internet; anything from a website to a Page or timeline on Facebook. For example, if you are writing a story, you might include a link to a blog you are referencing or a link to the blogger's Facebook timeline. If someone clicks on a link to another person's timeline, they'll only see the things that they are allowed to see.

A tag is a special type of link to someone's timeline that suggests that the tagged person add your story to their timeline. In cases where the tagged person isn't included in the audience of the story, it will add them so they can see it. Anyone can tag you in anything. Once you are tagged, you and your friends will be able to see it (such as in News Feed or in search).

You can choose whether a story you've been tagged in appears on your timeline. You can either approve each story individually or approve all stories by your friends. If you approve a story and later change your mind, you can always remove it from your timeline.

If you do not want someone to tag you, we encourage you to reach out to them and give them that feedback. If that does not work, you can block them. This will prevent them from tagging you going forward.

☞ Social reporting is a way for people to quickly and easily ask for help from someone they trust. Learn more at:

https://www.facebook.com/note.php?note_id=196124227075034&_ad=3&_at=iframe

☞ If you are linked to ~~or tagged~~ in a private space (such as a message or a group) only the people who can see the private space can see the link ~~or tag~~. Similarly, if you are linked to ~~or tagged~~ in a comment, only the people who can see the comment can see the link ~~or tag~~.

Other information

As described in the "what your friends and others share about you" section of this policy, your friends and others may share information about you. They may share photos or other information about you and tag you in their posts. If you do not like a particular post, tell them or report the post.

Groups

Once you are in a Group, anyone in that Group can add you to a subgroup. When someone adds you to a Group, you will be listed as "invited" until you visit the Group. You can always leave a Group, which will prevent others from adding you to it again.

Pages

Facebook Pages are public pages. Companies use Pages to share information about their products. Celebrities use Pages to talk about their latest projects. And communities use Pages to discuss topics of interest, everything from baseball to the opera.

Because Pages are public, information you share with a Page is public information. This means, for example, that if you post a comment on a Page, that comment may be used by the Page owner off Facebook, and anyone can see it.

When you "like" a Page, you create a connection to that Page. The connection is added to your timeline and your friends may see it in their News Feeds. You may be contacted by or receive updates from the Page, such as in your News Feed and your messages. You can remove the Pages you've "liked" through your timeline or on the Page.

Some Pages contain content that comes directly from the Page owner. Page owners can do this through online plugins, such as an iframe, and it works just like the games and other applications you use through Facebook. Because this content comes directly from the Page owner, that Page may be able to collect information about you, just like any website.

- ❖ Page administrators may have access to insights data, which will tell them generally about the people that visit their Page (as opposed to information about specific people). They may also know when you've made a connection to their Page because you've liked their Page or posted a comment.
- ❖ To control who can see the Facebook Pages you've liked, visit our Help Center.

III. Other websites and applications

About Facebook Platform

Facebook Platform (or simply Platform) refers to the way we help you share your information with the games, applications, and websites you and your friends use. Facebook Platform also lets you bring your friends with you, so you can connect with them off of Facebook. In these two ways, Facebook Platform helps you make your experiences on the web more personalized and social.

❖ Remember that these games, applications and websites are created and maintained by other businesses and developers who are not part of, or controlled by, Facebook, so you should always make sure to read their terms of service and privacy policies to understand how they treat your data.

Controlling what information you share with applications

When you connect with a game, application or website - such as by going to a game, logging in to a website using your Facebook account, or adding an app to your timeline - we give the game, application, or website (sometimes referred to as just "Applications" or "Apps") your

basic info (we sometimes call this your "public profile"), which includes your User ID and your public information. We also give them your friends' User IDs (also called your friend list) as part of your basic info.

Your friend list helps the application make your experience more social because it lets you find your friends on that application. Your User ID helps the application personalize your experience because it can connect your account on that application with your Facebook account, and it can access your basic info, which includes your public information and friend list. This includes the information you choose to make public, as well as information that is always publicly available. If the application needs additional information, such as your stories, photos or likes, it will have to ask you for specific permission.

The "Apps you use" setting lets you control the applications you use. You can see the permissions you have given these applications, the last time an application accessed your information, and the audience on Facebook for timeline stories and activity the application posts on your behalf. You can also remove applications you no longer want, or turn off all Platform applications. When you turn all Platform applications off, your User ID is no longer given to applications, even when your friends use those applications. But you will no longer be able to use any games, applications or websites through Facebook.

When you first visit an app, Facebook lets the app know your language, your country, and whether you are in an age group, for instance, under 18, between 18-20, or 21 and over. Age range lets apps provide you with age-appropriate content. If you install the app, it can access, store and update the information you've shared. Apps you've installed can update their records of your basic info, age range, language and country. ...if you haven't used an app in a while, you should consider removing it. Once you remove an app, it won't be able to continue to update the additional information you've given them permission to access, but it may still hold the information you have already shared. You always can contact the app directly and request that they delete your data. Learn more at: <https://www.facebook.com/help/how-apps-work>

⚡ Sometimes a game console, mobile phone, or other device might ask for permission to share specific information with the games and applications you use on that device. If you say okay, those applications will not be able to access any other information about you without asking specific permission from you or your friends.

⚡ Sites and apps that use Instant Personalization receive your User ID and friend list when you visit them.

⚡ You always can remove apps you've installed by using your app settings at: <https://www.facebook.com/settings/?tab=applications>. But remember, apps may still be able to access your information when the people you share with use them. And, if you've removed an application and want ~~them~~ it to delete the information you've already shared with ~~it~~ them, you should contact the application ~~and ask them to delete it~~. Visit the application's page on Facebook or ~~their~~ its own website to learn more about the app. For example, Apps may have reasons (e.g. legal obligations) to retain some data that you share with them.

Controlling what is shared when the people you share with use applications

Just like when you share information by email or elsewhere on the web, information you share on Facebook can be re-shared. This means that if you share something on Facebook, anyone who can see it can share it with others, including the games, applications, and websites they use.

Your friends and the other people you share information with often want to share your information with applications to make their experiences on those applications more personalized and social. For example, one of your friends might want to use a music application that allows them to see what their friends are listening to. To get the full benefit of that application, your friend would want to give the application her friend list – which includes your User ID – so the application knows which of her friends is also using it. Your friend might also want to share the music you “like” on Facebook. If you have made that information public, then the application can access it just like anyone else. But if you’ve shared your likes with just your friends, the application could ask your friend for permission to share them.

You can control most of the information other people can share with applications they use from the “~~Ads, Apps and Websites~~ App” settings page. But these controls do not let you limit access to your public information and friend list.

If you want to completely block applications from getting your information when your friends and others use them, you will need to turn off all Platform applications. This means that you will no longer be able to use any third-party Facebook-integrated games, applications or websites.

- ☞ If an application asks permission from someone else to access your information, the application will be allowed to use that information only in connection with the person that gave the permission, and no one else.
- ☞ For example, some apps use information such as your friends list, to personalize your experience or show you which of your friends use that particular app.

Logging in to another site using Facebook

Facebook Platform lets you log into other applications and websites using your Facebook account. When you log in using Facebook, we give the site your User ID (just like when you connect with any other application), but we do not share your email address or password with that website through this process without your permission.

If you already have an account on that website, the site may also be able to connect that account with your Facebook account. Sometimes it does this using what is called an “email hash”, which is similar to searching for someone on Facebook using an email address. Only the email addresses in this case are hashed so no email addresses are actually shared between Facebook and the website.

How it works

The website sends over a hashed version of your email address, and we match it with a database of email addresses that we have also hashed. If there is a match, then we tell the website the User ID associated with the email address. This way, when you log into the website using Facebook, the website can link your Facebook account to your account on that website.

About social plugins

Social plugins are buttons, boxes, and stories (such as the Like button) that other websites can use to present Facebook content to you and create more social and personal experiences for you. While you view these buttons, boxes, and stories on other sites, the content comes directly from Facebook.

Sometimes plugins act just like applications. You can spot one of these plugins because it will ask you for permission to access your information or to publish information back to Facebook. For example, if you use a registration plugin on a website, the plugin will ask your permission to share your basic info with the website to make it easier for you to register for the website. Similarly, if you use an "Add To Timeline" plugin, the plugin will ask for your permission to publish stories about your activities on that website to Facebook.

If you make something public using a plugin, such as posting a public comment on a newspaper's website, then that website can access your comment (along with your User ID) just like everyone else.

⚡ If you post something using a social plugin and you do not see a sharing icon, you should assume that story is Public. For example, if you post a comment through a Facebook comment plugin on a site, your story is Public, and everyone, including the website, can see your story.

⚡ Websites that use social plugins can sometimes tell that you have engaged with the social plugin. For example, they may know that you clicked on a Like button in a social plugin.

⚡ We receive data when you visit a site with a social plugin. We keep this data for a maximum of 90 days. After that, we remove your name or any other personally identifying information from the data, or combine it with other people's data in a way that it is no longer associated with you. Learn more at: <https://www.facebook.com/help/social-plugins>

About instant personalization

Instant personalization (sometimes also referred to as "Start now") is a way for Facebook to help partners (such as Bing and Rotten Tomatoes) on and off Facebook to create a more personalized and social experience for logged in users than a social plugin can offer. When you visit a site or app using instant personalization, it will know some information about you and your friends the moment you arrive. This is because sites and apps using instant personalization can access your User ID, your friend list, and your public information.

The first time you visit a site or app using instant personalization, you will see a notification letting you know that the site or app has partnered with Facebook to provide a personalized experience.

The notification will give you the ability to disable or turn off instant personalization for that site or app. If you do that, that site or app is required to delete all of the information about you it received from Facebook as part of the instant personalization program. In addition, we will prevent that site from accessing your information in the future, even when your friends use that site.

If you decide that you do not want to experience instant personalization for all partner sites and apps, you can disable instant personalization from the “~~Ads, Apps and Websites~~” settings page.

If you turn off instant personalization, these partner third party sites and apps will not be able to access your public information, even when your friends visit those sites.

⚠️ If you turn off an instant personalization site or app after you have been using it or visited it a few times (or after you have given it specific permission to access your data), it will not automatically delete information about you it received through Facebook. Like all other apps, the site is required by our policies to delete information about you if you ask it to do so.

How it works

To join the instant personalization program, a potential partner must enter into an agreement with us designed to protect your privacy. For example, this agreement requires that the partner delete information about you if you turn off instant personalization when you first visit the site or app. It also prevents the partner from accessing any information about you until you or your friends visit its site.

Instant personalization partners sometimes use an email hash process to see if any of their users are on Facebook and get those users' User IDs. This process is similar to searching for someone on Facebook using an email address, except in this case, the email addresses are hashed so no actual email addresses are exchanged. The partner is also contractually required not to use your User ID for any purpose (other than associating it with your account) until you or your friends visit the site.

When you visit a site or app using instant personalization, we provide the site or app with your User ID and your friend list (as well as your age range, locale, and gender). The site or app can then connect your account with ~~that partner with~~ your friends' accounts to make the site or app instantly social. The site can also access public information associated with any of the User IDs it receives, which it can use to make them instantly personalized. For example, if the site is a music site, it can access your music interests to suggest songs you may like, and access your friends' music interests to let you know what they are listening to. Of course it can only access

your or your friends' music interests if they are public. If the site or app wants any additional information, it will have to get your specific permission.

Public search engines

Your public search setting controls whether people who enter your name on a public search engine may see your public timeline (including in sponsored results). You can find your public search setting on the "Privacy Settings and Tools, Ads, Apps and Websites" settings page.

☞ This setting does not apply to search engines that access your information as an application using Facebook Platform.

☞ If you turn your public search setting off and then search for yourself on a public search engine, you may still see a preview of your timeline. This is because some search engines cache information for a period of time. You can learn more about how to request a search engine to remove you from cached information at: <https://www.facebook.com/help/?faq=13323>

IV. ~~How a~~Advertising and Facebook content and Sponsored Stories work

Advertising Personalized ads

Facebook offers a range of products that allow advertisers to reach people on and off Facebook.

When we deliver ads, we do not share your information (information that personally identifies you, such as your name or contact information) with advertisers unless you give us permission. We may provide advertisers with information when we have removed your name or other personally identifying information from it, or combined it with other information so that it no longer personally identifies you. For example, we may tell an advertiser how its ads perform or how many people viewed or clicked on their ads or install an app after seeing an ad.

So we can show you content that you may find interesting, we may use all of the information we receive about you to serve ads that are more relevant to you. For example, this includes:

- information you provide at registration or add to your account or timeline,
- things you share and do on Facebook, such as what you like, and your interactions with advertisements, partners, or apps,
- keywords from your stories, and
- things we infer from your use of Facebook.

For many ads we serve, advertisers may choose their audience by location, demographics, likes, keywords, and any other information we receive or infer about users. Here are some of the ways advertisers may target relevant ads:

- demographics and interests: for example, 18 to 35 year-old women who live in the United States and like basketball;

- topics or keywords: for example, "music" or people who like a particular song or artist;
- Page likes (including topics such as products, brands, religion, health status, or political views): for example, if you like a Page about Gluten-free food, you may receive ads about relevant food products; or
- categories (including things like "moviegoer" or a "sci-fi fan"): for example, if a person "likes" the "Star Trek" Page and mentions "Star Wars" when they check into a movie theater, we may infer that this person is likely to be a sci-fi fan and advertisers of sci-fi movies could ask us to target that category.

In addition to delivering relevant ads, Facebook sometimes pairs ads with social context, meaning stories about social actions that you or your friends have taken. For example, an ad for a sushi restaurant's Facebook Page may be paired with a News Feed story that one of your friends likes that Page.

We also sometimes serve these same types of ads on other sites or may serve just the social context (such as with ads served by others), so that the ads are more relevant to you. Just like any other content you share on Facebook, only people who you're already sharing with on Facebook would see it when it is paired with an ad. You can learn more about ads and social context, including the relevant settings and controls available to you, by visiting the Advertising on Facebook page.

We also allow advertisers to reach people on Facebook using the information they already have about you (such as email addresses or whether you have visited their websites previously).

🔗 In addition to the information we provide in this section, you can also learn more about advertising products, how they work, our partnerships, and the choices you have, by visiting our "Advertising on Facebook" page.

🔗 We require advertisers to comply with our Advertising Guidelines, including provisions relating to the use of sensitive data.

🔗 Advertisers and their partners sometimes use cookies or other similar technologies in order to serve and measure ads and to make their ads more effective. Learn more about cookies, pixels and similar technologies.

~~We do not share any of your information with advertisers (unless, of course, you give us permission). As described in this policy, we may share your information when we have removed from it anything that personally identifies you or combined it with other information so that it no longer personally identifies you.~~

~~We use the information we receive, including the information you provide at registration or add to your account or timeline, to deliver ads and to make them more relevant to you. This includes all of the things you share and do on Facebook, such as the Pages you like or key words~~

from your stories, and the things we infer from your use of Facebook. Learn more at: <https://www.facebook.com/help/?page=226611954016283>

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. We require advertisers to comply with our [Advertising Guidelines](#), including provisions relating to the use of sensitive data. Try this tool yourself to see one of the ways advertisers target ads and what information they see at: <https://www.facebook.com/ads/create/>

If the advertiser chooses to run the ad (also known as placing the order), we serve the ad to people who meet the criteria the advertiser selected, but we do not tell the advertiser who any of those people are. So, for example, if a person views or otherwise interacts with the ad, the advertiser might infer that the person is an 18 to 35 year old woman who lives in the U.S. and likes basketball. But we would not tell the advertiser who that person is.

After the ad runs, we provide advertisers with reports on how their ads performed. For example we give advertisers reports telling them how many users saw or clicked on their ads. But these reports are anonymous. We do not tell advertisers who saw or clicked on their ads.

🔍 Advertisers or their partners sometimes place cookies on your computer (or use other similar system technologies) in order to serve ads and to make their ads more effective. Learn more about [cookies, pixels and other system technologies](#).

🔍 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.

Ads + social context

Facebook Ads are sometimes paired with social actions your friends have taken. For example, an ad for a sushi restaurant may be paired with a news story that one of your friends likes that restaurant's Facebook page.

~~This is the same type of news story that could show up in your News Feed, only we place it next to a paid advertisement to make that ad more relevant and interesting.~~

~~When you show up in one of these news stories, we will only pair it with ads shown to your friends. If you do not want to appear in stories paired with Facebook Ads, you can opt out using your "Edit social ads" setting.~~

~~🔍 Learn what happens when you click "Like" on an advertisement or an advertiser's Facebook Page at: <https://www.facebook.com/help/?faq=19399>~~

~~🔍 We may serve ads, including those with social context (or serve just social context), on other sites. These work just like the ads we serve on Facebook—the advertisers do not receive any of your information. Only people that could see the Facebook action (like on your timeline) would see it paired in this way.~~

~~🔍 Your "Show my social actions in Facebook Ads" setting only controls ads with social context. It does not control Sponsored Stories, ads or information about Facebook's services and features, or other Facebook content.~~

~~🔍 Games, applications and websites can serve ads directly to you or help us serve ads to you or others if they have information like your User ID or email address.~~

Sponsored stories

~~Many of the things you do on Facebook (like "liking" a Page) are posted to your timeline and shared in News Feed. But there's a lot to read in News Feed. That's why we allow people to "sponsor" your stories to make sure your friends and subscribers see them. For example, if you RSVP to an event hosted by a local restaurant, that restaurant may want to make sure your friends see it so they can come too.~~

~~If they do sponsor a story, that story will appear in the same place ads usually do or in your News Feed under the heading "Sponsored" or something similar. Only people that could originally see the story can see the sponsored story, and no personal information about you (or your friends) is shared with the sponsor.~~

~~🔍 Your "Show my social actions in Facebook Ads" setting only controls ads with social context. It does not control Sponsored Stories, ads or information about Facebook's services and features, or other Facebook content.~~

Facebook content

We like to tell you about some of the features and tools your friends and others use on Facebook, to help you have a better experience. For example, if your friend uses our friend finder tool to find more friends on Facebook, we may tell you about it to encourage you to use it as well. This of course means your friend may similarly see suggestions based on the things you do. But we will try to only show it to friends that could benefit from your experience.

~~Your "Show my social actions in Facebook Ads" setting only controls ads with social context. It does not control Sponsored Stories, ads or information about Facebook's services and features, or other Facebook content~~

V. Cookies, pixels and other similar technologies

Cookies are small pieces of data that are stored on your computer, mobile phone or other device. Pixels are small blocks of code on webpages that do things like allow another server to measure viewing of a webpage and often are used in connection with cookies.

We use technologies like cookies, pixels, and local storage (like on your browser or device, which is similar to a cookie but holds more information) to provide and understand a range of products and services. Learn more at: <https://www.facebook.com/help/cookies>

We use these technologies to do things like:

- make Facebook easier or faster to use;
- enable features and store information about you (including on your device or in your browser cache) and your use of Facebook;
- deliver, understand and improve advertising;
- monitor and understand the use of our products and services; and,
- ~~to~~ protect you, others and Facebook.

For example, we may use ~~these tools~~ ~~them~~ to know you are logged in to Facebook, to help you use social plugins and share buttons, or to know when you are interacting with our advertising or Platform partners.

We may ask advertisers or other partners to serve ads or services to computers, mobile phones or other devices, which may use a cookie, pixel or other similar technology placed by Facebook or the third party (although we would not share ~~any other~~ information that personally identifies you with an advertiser).

Most companies on the web use cookies (or other similar technological tools), including our advertising and Platform partners. For example, our Platform partners, advertisers or Page administrators may use cookies or similar technologies when you access their apps, ads, Pages or other content.

☞ Cookies and things like local storage help make Facebook work, like allowing pages to load faster because certain content is stored on your browser or by helping us authenticate you to deliver personalized content.

☞ To learn more about how advertisers generally use cookies and the choices advertisers provide, visit the Network Advertising Initiative at http://www.networkadvertising.org/managing/opt_out.asp, the Digital Advertising Alliance at

<http://www.aboutads.info/>, the Internet Advertising Bureau (US) at <http://www.iab.net> or the Internet Advertising Bureau (EU) at <http://youronlinechoices.eu/>.

☞ Refer to your browser or device's help material to learn what controls you can often use to remove or block cookies or other similar technologies or block or remove other data stored on your computer or device (such as by using the various settings in your browser). If you do this, it may affect your ability to use Facebook or other websites and apps.

VI. Some other things you need to know

Safe harbor

Facebook complies with the U.S.-EU and U.S.-Swiss Safe Harbor frameworks as set forth by the Department of Commerce regarding the collection, use, and retention of data from the European Union. To view our certification, visit the U.S. Department of Commerce's Safe Harbor website at: <https://safeharbor.export.gov/list.aspx>. As part of our participation in the Safe Harbor program, we agree to resolve disputes you have with us in connection with our policies and practices through TRUSTe. If you would like to contact TRUSTe, visit: <https://feedback-form.truste.com/watchdog/request>

Contact us with questions or disputes

If you have questions or complaints regarding our Data Use Policy or practices, please contact us by mail at 1601 Willow Road, Menlo Park, CA 94025 if you reside in the U.S. or Canada, or at Facebook Ireland Ltd., Hanover Reach, 5-7 Hanover Quay, Dublin 2 Ireland if you live outside the U.S. or Canada. Anyone may also contact us through this help page: https://www.facebook.com/help/contact_us.php?id=173545232710000

Responding to legal requests and preventing harm

We may access, preserve and share your information in response to a legal request (like a search warrant, court order or subpoena) if we have a good faith belief that the law requires us to do so. This may include responding to legal requests from jurisdictions outside of the United States where we have a good faith belief that the response is required by law in that jurisdiction, affects users in that jurisdiction, and is consistent with internationally recognized standards. We may also access, preserve and share information when we have a good faith belief it is necessary to: detect, prevent and address fraud and other illegal activity; to protect ourselves, you and others, including as part of investigations; ~~or, and~~ to prevent death or imminent bodily harm.

Information we receive about you, including financial transaction data related to purchases made with Facebook Credits, may be accessed, processed and retained for an extended period of time when it is the subject of a legal request or obligation, governmental investigation, or investigations concerning possible violations of our terms or policies, or otherwise to prevent harm. We also may retain information from accounts disabled for violations of our terms for at least a year to prevent repeat abuse or other violations of our terms.

Access requests

You can access and correct most of your personal data stored by Facebook by logging into your account and viewing your timeline and activity log. You can also download a copy of your personal data by visiting your "[Account Settings](#)" ([General Account Settings page](#)), clicking on "Download a copy of your Facebook data" and then clicking on the link for your expanded archive. Learn more at: <https://www.facebook.com/help/?faq=226281544049399>

Notifications and Other Messages

We may send you notifications and other messages using the contact information we have for you, like your email address. You can control most of the notifications you receive, including ones from Pages you like and applications you use, using controls we provide, such as a control included in the email you receive or in your "Notifications" settings.

Friend Finder

We offer tools to help you upload your friends' contact information so that you and others can find friends on Facebook, and invite friends who do not use Facebook to join, and so we can offer you and others better experiences on Facebook through suggestions and other customized experiences. If you do not want us to store this information, visit this help page at: https://www.facebook.com/contact_importer/remove_uploads.php.

If you give us your password, we will delete it after you upload your friends' contact information.

Invitations

When you invite a friend to join Facebook, we send a message on your behalf using your name, and we may also include names and pictures of other people your friend might know on Facebook. We'll also send a few reminders to those you invite, but the invitation will also give your friend the opportunity to opt out of receiving other invitations to join Facebook.

Memorializing accounts

We may memorialize the account of a deceased person. When we memorialize an account, we keep the timeline on Facebook, but limit access and some features. You can report a deceased person's timeline at: https://www.facebook.com/help/contact.php?show_form=deceased
We also may close an account if we receive a formal request that satisfies certain criteria.

Affiliates

We may share information we receive with businesses that are legally part of the same group of companies that Facebook is part of, or that become part of that group (often these companies are called affiliates). Likewise, our affiliates may share information with us as well. This sharing is done in compliance with applicable laws including where such applicable laws require consent. We and our affiliates may use shared information to help provide, understand, and improve our services and their own services.

Service Providers

We give your information to the people and companies that help us provide, understand and improve the services we offer. For example, we may use outside vendors to help host our website, serve photos and videos, process payments, analyze data, conduct and publish research, measure the effectiveness of ads, or provide search results. In some cases we provide the service jointly with another company, such as the Facebook Marketplace. In all of these cases our partners must agree to only use your information consistent with the agreement we enter into with them, as well as this Data Use Policy.

Security and bugs

We do our best to keep your information secure, but we need your help. For more detailed information about staying safe on Facebook, visit the [Facebook Security Page](#). We try to keep Facebook up, bug-free and safe, but can't make guarantees about any part of our services or products.

Change of Control

If the ownership of our business changes, we may transfer your information to the new owner so they can continue to operate the service. But they will still have to honor the commitments we have made in this Data Use Policy.

Notice of Changes

If we make changes to this Data Use Policy we will notify you (for example, by publication here and on the [Facebook Site Governance Page](#)). If the changes are material, we will provide you additional, prominent notice as appropriate under the circumstances. You can make sure that you receive notice directly by liking the [Facebook Site Governance Page](#).

Opportunity to comment

Unless we make a change for legal or administrative reasons, or to correct an inaccurate statement, we will give you seven (7) days to provide us with comments on the change. After the comment period, if we adopt any changes, we will provide notice (for example, on the [Facebook Site Governance Page](#) or in this policy) of the effective date.

Information for users outside of the United States and Canada

Company Information: The website under www.facebook.com and the services on these pages are being offered to users outside of the U.S. and Canada by Facebook Ireland Ltd., Hanover Reach, 5-7 Hanover Quay, Dublin 2 Ireland. The company Facebook Ireland Ltd. has been established and registered in Ireland as a private limited company, Company Number: 462932, and is the data controller responsible for your personal information.

Directors: Sonia Flynn (Irish), Shane Crehan (Irish).

Your California privacy rights

California law permits residents of California to request certain details about what personal information a company shares with third parties for the third parties' direct marketing purposes. Facebook does not share your information with third parties for the third parties'

own and independent direct marketing purposes unless we receive your permission. Learn more about the [information we receive and how it is used](#) and [other websites and applications](#). If you have questions about our sharing practices or your rights under California law, please write us at 1601 Willow Road, Menlo Park, CA 94025 or contact us through this help page: https://www.facebook.com/help/contact_us.php?id=173545232710000

This agreement was written in English (US). To the extent any translated version of this agreement conflicts with the English version, the English version controls. Please note that Section 17 contains certain changes to the general terms for users outside the United States.

Date of Last Revision: ~~December 11, 2012~~ September ##, 2013.

Statement of Rights and Responsibilities

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 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.

1. Privacy

Your privacy is very important to us. We designed our [Data Use Policy](#) 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.

2. Sharing Your Content and Information

You own all of the content and information you post on Facebook, and you can control how it is shared through your [privacy](#) and [application settings](#). In addition:

1. For content that is covered by intellectual property rights, like photos and videos (IP content), you specifically give us the following permission, subject to your [privacy](#) and [application settings](#): you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (IP License). This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it.
2. When you delete IP content, it is deleted in a manner similar to emptying the recycle bin on a computer. However, you understand that removed content may persist in backup copies for a reasonable period of time (but will not be available to others).
3. When you use an application, the application may ask for your permission to access your content and information as well as content and information that others have shared with you. We require applications to respect your privacy, and your agreement with that application will control how the application can use, store, and transfer that content and information. (To learn more about Platform, including how you can control what information other people may share with applications, read our [Data Use Policy](#) and [Platform Page](#).)

4. When you publish content or information using the Public setting, it means that you are allowing everyone, including people off of Facebook, to access and use that information, and to associate it with you (i.e., your name and profile picture).
5. We always appreciate your feedback or other suggestions about Facebook, but you understand that we may use them without any obligation to compensate you for them (just as you have no obligation to offer them).

3. Safety

We do our best to keep Facebook safe, but we cannot guarantee it. We need your help to keep Facebook safe, which includes the following commitments by you:

1. You will not post unauthorized commercial communications (such as spam) on Facebook.
2. You will not collect users' content or information, or otherwise access Facebook, using automated means (such as harvesting bots, robots, spiders, or scrapers) without our prior permission.
3. You will not engage in unlawful multi-level marketing, such as a pyramid scheme, on Facebook.
4. You will not upload viruses or other malicious code.
5. You will not solicit login information or access an account belonging to someone else.
6. You will not bully, intimidate, or harass any user.
7. You will not post content that: is hate speech, threatening, or pornographic; incites violence; or contains nudity or graphic or gratuitous violence.
8. You will not develop or operate a third-party application containing alcohol-related, dating or other mature content (including advertisements) without appropriate age-based restrictions.
9. You will follow our [Promotions Guidelines](#) and all applicable laws if you publicize or offer any contest, giveaway, or sweepstakes ("promotion") on Facebook.
10. You will not use Facebook to do anything unlawful, misleading, malicious, or discriminatory.
11. You will not do anything that could disable, overburden, or impair the proper working or appearance of Facebook, such as a denial of service attack or interference with page rendering or other Facebook functionality.
12. You will not facilitate or encourage any violations of this Statement or our policies.

4. Registration and Account Security

Facebook users provide their real names and information, and we need your help to keep it that way. Here are some commitments you make to us relating to registering and maintaining the security of your account:

1. You will not provide any false personal information on Facebook, or create an account for anyone other than yourself without permission.
2. You will not create more than one personal account.
3. If we disable your account, you will not create another one without our permission.
4. You will not use your personal timeline primarily for your own commercial gain, and will use a Facebook Page for such purposes.
5. You will not use Facebook if you are under 13.
6. You will not use Facebook if you are a convicted sex offender.
7. You will keep your contact information accurate and up-to-date.
8. You will not share your password (or in the case of developers, your secret key), let anyone else access your account, or do anything else that might jeopardize the security of your account.
9. You will not transfer your account (including any Page or application you administer) to anyone without first getting our written permission.
10. If you select a username or similar identifier for your account or Page, we reserve the right to remove or reclaim it if we believe it is appropriate (such as when a trademark owner complains about a username that does not closely relate to a user's actual name).

5. Protecting Other People's Rights

We respect other people's rights, and expect you to do the same.

1. You will not post content or take any action on Facebook that infringes or violates someone else's rights or otherwise violates the law.
2. We can remove any content or information you post on Facebook if we believe that it violates this Statement or our policies.
3. We provide you with tools to help you protect your intellectual property rights. To learn more, visit our [How to Report Claims of Intellectual Property Infringement](#) page.
4. If we remove your content for infringing someone else's copyright, and you believe we removed it by mistake, we will provide you with an opportunity to appeal.
5. If you repeatedly infringe other people's intellectual property rights, we will disable your account when appropriate.
6. You will not use our copyrights or trademarks (including Facebook, the Facebook and F Logos, FB, Face, Poke, Book and Wall), or any confusingly similar marks, except as expressly permitted by our Brand Usage Guidelines or with our prior written permission.
7. If you collect information from users, you will: obtain their consent, make it clear you (and not Facebook) are the one collecting their information, and post a privacy policy explaining what information you collect and how you will use it.
8. You will not post anyone's identification documents or sensitive financial information on Facebook.

9. You will not tag users or send email invitations to non-users without their consent. Facebook offers social reporting tools to enable users to provide feedback about tagging.

6. **Mobile and Other Devices**

1. We currently provide our mobile services for free, but please be aware that your carrier's normal rates and fees, such as text messaging and data charges-fees, will still apply.
2. In the event you change or deactivate your mobile telephone number, you will update your account information on Facebook within 48 hours to ensure that your messages are not sent to the person who acquires your old number.
3. You provide consent and all rights necessary to enable users to sync (including through an application) their devices with any information that is visible to them on Facebook.

7. **Payments**

If you make a payment on Facebook or use Facebook Credits, you agree to our Payments Terms.

8. **Special Provisions Applicable to Social Plugins**

If you include our Social Plugins, such as the Share or Like buttons on your website, the following additional terms apply to you:

1. We give you permission to use Facebook's Social Plugins so that users can post links or content from your website on Facebook.
2. You give us permission to use and allow others to use such links and content on Facebook.
3. You will not place a Social Plugin on any page containing content that would violate this Statement if posted on Facebook.

9. **Special Provisions Applicable to Developers/Operators of Applications and Websites**

If you are a developer or operator of a Platform application or website, the following additional terms apply to you:

1. You are responsible for your application and its content and all uses you make of Platform. This includes ensuring your application or use of Platform meets our Facebook Platform Policies and our Advertising Guidelines.
2. Your access to and use of data you receive from Facebook, will be limited as follows:
 1. You will only request data you need to operate your application.
 2. You will have a privacy policy that tells users what user data you are going to use and how you will use, display, share, or transfer that data and you will include your privacy policy URL in the Developer Application.

3. You will not use, display, share, or transfer a user's data in a manner inconsistent with your privacy policy.
4. You will delete all data you receive from us concerning a user if the user asks you to do so, and will provide a mechanism for users to make such a request.
5. You will not include data you receive from us concerning a user in any advertising creative.
6. You will not directly or indirectly transfer any data you receive from us to (or use such data in connection with) any ad network, ad exchange, data broker, or other advertising related toolset, even if a user consents to that transfer or use.
7. You will not sell user data. If you are acquired by or merge with a third party, you can continue to use user data within your application, but you cannot transfer user data outside of your application.
8. We can require you to delete user data if you use it in a way that we determine is inconsistent with users' expectations.
9. We can limit your access to data.
10. You will comply with all other restrictions contained in our [Facebook Platform Policies](#).
3. You will not give us information that you independently collect from a user or a user's content without that user's consent.
4. You will make it easy for users to remove or disconnect from your application.
5. You will make it easy for users to contact you. We can also share your email address with users and others claiming that you have infringed or otherwise violated their rights.
6. You will provide customer support for your application.
7. You will not show third party ads or web search boxes on www.facebook.com.
8. We give you all rights necessary to use the code, APIs, data, and tools you receive from us.
9. You will not sell, transfer, or sublicense our code, APIs, or tools to anyone.
10. You will not misrepresent your relationship with Facebook to others.
11. You may use the logos we make available to developers or issue a press release or other public statement so long as you follow our [Facebook Platform Policies](#).
12. We can issue a press release describing our relationship with you.
13. You will comply with all applicable laws. In particular you will (if applicable):
 1. have a policy for removing infringing content and terminating repeat infringers that complies with the Digital Millennium Copyright Act.
 2. comply with the Video Privacy Protection Act (VPPA), and obtain any opt-in consent necessary from users so that user data subject to the VPPA may be shared on Facebook. You represent that any disclosure to us will not be incidental to the ordinary course of your business.
14. We do not guarantee that Platform will always be free.

15. You give us all rights necessary to enable your application to work with Facebook, including the right to incorporate content and information you provide to us into streams, timelines, and user action stories.
16. You give us the right to link to or frame your application, and place content, including ads, around your application.
17. We can analyze your application, content, and data for any purpose, including commercial (such as for targeting the delivery of advertisements and indexing content for search).
18. To ensure your application is safe for users, we can audit it.
19. We can create applications that offer similar features and services to, or otherwise compete with, your application.

10. About Advertisements and Other Commercial Content Served or Enhanced by Facebook

Our goal is to deliver advertisings and other commercial or sponsored content that are-is valuable to our users and advertisers. In order to help us do that, you agree to the following:

1. ~~You can use your privacy settings to limit how your name and profile picture may be associated with commercial, sponsored, or related content (such as a brand you like) served or enhanced by us.~~ You give us permission to use your name, and profile picture, content, and information in connection with commercial, sponsored, or related that content (such as a brand you like) served or enhanced by us, subject to the limits you place. This means, for example, that you permit a business or other entity to pay us to display your name and/or profile picture with your content or information, without any compensation to you. If you have selected a specific audience for your content or information, we will respect your choice when we use it.

If you are under the age of eighteen (18), or under any other applicable age of majority, you represent that at least one of your parents or legal guardians has also agreed to the terms of this section (and the use of your name, profile picture, content, and information) on your behalf.

2. We do not give your content or information to advertisers without your consent.
3. You understand that we may not always identify paid services and communications as such.

11. Special Provisions Applicable to Advertisers

You can target your desired audience by buying ads on Facebook or our publisher network. The following additional terms apply to you if you place an order through our online advertising portal (Order):

1. When you place an Order, you will tell us the type of advertising you want to buy, the amount you want to spend, and your bid. If we accept your Order, we will deliver your ads as inventory becomes available. When serving your ad, we do our best to deliver the ads to the audience you specify, although we cannot guarantee in every instance that your ad will reach its intended target.
2. In instances where we believe doing so will enhance the effectiveness of your advertising campaign, we may broaden the targeting criteria you specify.
3. You will pay for your Orders in accordance with our [Payments Terms](#). The amount you owe will be calculated based on our tracking mechanisms.
4. Your ads will comply with our [Advertising Guidelines](#).
5. We will determine the size, placement, and positioning of your ads.
6. We do not guarantee the activity that your ads will receive, such as the number of clicks your ads will get.
7. We cannot control how clicks are generated on your ads. We have systems that attempt to detect and filter certain click activity, but we are not responsible for click fraud, technological issues, or other potentially invalid click activity that may affect the cost of running ads.
8. You can cancel your Order at any time through our online portal, but it may take up to 24 hours before the ad stops running. You are responsible for paying for all ads that run.
9. Our license to run your ad will end when we have completed your Order. You understand, however, that if users have interacted with your ad, your ad may remain until the users delete it.
10. We can use your ads and related content and information for marketing or promotional purposes.
11. You will not issue any press release or make public statements about your relationship with Facebook without our prior written permission.
12. We may reject or remove any ad for any reason.
13. If you are placing ads on someone else's behalf, you must have permission to place those ads, including the following:
 1. You warrant that you have the legal authority to bind the advertiser to this Statement.
 2. You agree that if the advertiser you represent violates this Statement, we may hold you responsible for that violation.

12. Special Provisions Applicable to Pages

If you create or administer a Page on Facebook, or run a promotion or an offer from your Page, you agree to our [Pages Terms](#).

13. Special Provisions Applicable to Software

1. If you download or use our software, such as a stand-alone software product, an app, or a browser plugin, you agree that from time to time, the software may

download and install upgrades, updates and additional features from us in order to improve, enhance, and further develop the software.

2. You will not modify, create derivative works of, decompile, or otherwise attempt to extract source code from us, unless you are expressly permitted to do so under an open source license, or we give you express written permission.

14. Amendments

1. Unless we make a change for legal or administrative reasons, or to correct an inaccurate statement, we will provide you with seven (7) days notice (for example, by posting the change on the Facebook Site Governance Page) and an opportunity to comment on changes to this Statement. You can also visit our Facebook Site Governance Page and "like" the Page to get updates about changes to this Statement.
2. If we make changes to policies referenced in or incorporated by this Statement, we may provide notice on the Site Governance Page.
3. Your continued use of Facebook following changes to our terms constitutes your acceptance of our amended terms.

15. Termination

If you violate the letter or spirit of this Statement, or otherwise create risk or possible legal exposure for us, we can stop providing all or part of Facebook to you. We will notify you by email or at the next time you attempt to access your account. You may also delete your account or disable your application at any time. In all such cases, this Statement shall terminate, but the following provisions will still apply: 2.2, 2.4, 3-5, 8.2, 9.1-9.3, 9.9, 9.10, 9.13, 9.15, 9.18, 10.3, 11.2, 11.5, 11.6, 11.9, 11.12, 11.13, and 15-19.

16. Disputes

1. You will resolve any claim, cause of action or dispute (claim) you have with us arising out of or relating to this Statement or Facebook exclusively in the U.S. District Court for the Northern District of California or a state or federal court located in Santa MateoClara County, and you agree to submit to the personal jurisdiction of such courts for the purpose of litigating all such claims. The laws of the State of California will govern this Statement, as well as any claim that might arise between you and us, without regard to conflict of law provisions. ~~You agree to submit to the personal jurisdiction of the courts located in Santa Clara County, California for the purpose of litigating all such claims.~~
2. If anyone brings a claim against us related to your actions, content or information on Facebook, you will indemnify and hold us harmless from and against all damages, losses, and expenses of any kind (including reasonable legal fees and costs) related to such claim. Although we provide rules for user conduct, we do not control or direct users' actions on Facebook and are not responsible for the content or information users transmit or share on Facebook. We are not responsible for any offensive, inappropriate, obscene, unlawful or

otherwise objectionable content or information you may encounter on Facebook. We are not responsible for the conduct, whether online or offline, or any user of Facebook.

3. WE TRY TO KEEP FACEBOOK UP, BUG-FREE, AND SAFE, BUT YOU USE IT AT YOUR OWN RISK. WE ARE PROVIDING FACEBOOK AS IS WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. WE DO NOT GUARANTEE THAT FACEBOOK WILL ALWAYS BE SAFE, SECURE OR ERROR-FREE OR THAT FACEBOOK WILL ALWAYS FUNCTION WITHOUT DISRUPTIONS, DELAYS OR IMPERFECTIONS. FACEBOOK IS NOT RESPONSIBLE FOR THE ACTIONS, CONTENT, INFORMATION, OR DATA OF THIRD PARTIES, AND YOU RELEASE US, OUR DIRECTORS, OFFICERS, EMPLOYEES, AND AGENTS FROM ANY CLAIMS AND DAMAGES, KNOWN AND UNKNOWN, ARISING OUT OF OR IN ANY WAY CONNECTED WITH ANY CLAIM YOU HAVE AGAINST ANY SUCH THIRD PARTIES. IF YOU ARE A CALIFORNIA RESIDENT, YOU WAIVE CALIFORNIA CIVIL CODE §1542, WHICH SAYS: A GENERAL RELEASE DOES NOT EXTEND TO CLAIMS WHICH THE CREDITOR DOES NOT KNOW OR SUSPECT TO EXIST IN HIS FAVOR AT THE TIME OF EXECUTING THE RELEASE, WHICH IF KNOWN BY HIM MUST HAVE MATERIALLY AFFECTED HIS SETTLEMENT WITH THE DEBTOR. WE WILL NOT BE LIABLE TO YOU FOR ANY LOST PROFITS OR OTHER CONSEQUENTIAL, SPECIAL, INDIRECT, OR INCIDENTAL DAMAGES ARISING OUT OF OR IN CONNECTION WITH THIS STATEMENT OR FACEBOOK, EVEN IF WE HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. OUR AGGREGATE LIABILITY ARISING OUT OF THIS STATEMENT OR FACEBOOK WILL NOT EXCEED THE GREATER OF ONE HUNDRED DOLLARS (\$100) OR THE AMOUNT YOU HAVE PAID US IN THE PAST TWELVE MONTHS. APPLICABLE LAW MAY NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY OR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU. IN SUCH CASES, FACEBOOK'S LIABILITY WILL BE LIMITED TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW.

17. Special Provisions Applicable to Users Outside the United States

We strive to create a global community with consistent standards for everyone, but we also strive to respect local laws. The following provisions apply to users and non-users who interact with Facebook outside the United States:

1. You consent to having your personal data transferred to and processed in the United States.
2. If you are located in a country embargoed by the United States, or are on the U.S. Treasury Department's list of Specially Designated Nationals you will not engage in commercial activities on Facebook (such as advertising or payments) or operate a Platform application or website. You will not use Facebook if you are prohibited from receiving products, services, or software originating from the United States.

3. Certain specific terms that apply only for German users are available [here](#).

18. Definitions

1. By "Facebook" we mean the features and services we make available, including through (a) our website at www.facebook.com and any other Facebook branded or co-branded websites (including sub-domains, international versions, widgets, and mobile versions); (b) our Platform; (c) social plugins such as the Like button, the Share button and other similar offerings and (d) other media, software (such as a toolbar), devices, or networks now existing or later developed.
2. By "Platform" we mean a set of APIs and services (such as content) that enable others, including application developers and website operators, to retrieve data from Facebook or provide data to us.
3. By "information" we mean facts and other information about you, including actions taken by users and non-users who interact with Facebook.
4. By "content" we mean anything you or other users post on Facebook that would not be included in the definition of information.
5. By "data" or "user data" or "user's data" we mean any data, including a user's content or information that you or third parties can retrieve from Facebook or provide to Facebook through Platform.
6. By "post" we mean post on Facebook or otherwise make available by using Facebook.
7. By "use" we mean use, run, copy, publicly perform or display, distribute, modify, translate, and create derivative works of.
8. By "active registered user" we mean a user who has logged into Facebook at least once in the previous 30 days.
9. By "application" we mean any application or website that uses or accesses Platform, as well as anything else that receives or has received data from us. If you no longer access Platform but have not deleted all data from us, the term application will apply until you delete the data.

19. Other

1. If you are a resident of or have your principal place of business in the US or Canada, this Statement is an agreement between you and Facebook, Inc. Otherwise, this Statement is an agreement between you and Facebook Ireland Limited. References to "us," "we," and "our" mean either Facebook, Inc. or Facebook Ireland Limited, as appropriate.
2. This Statement makes up the entire agreement between the parties regarding Facebook, and supersedes any prior agreements.
3. If any portion of this Statement is found to be unenforceable, the remaining portion will remain in full force and effect.
4. If we fail to enforce any of this Statement, it will not be considered a waiver.
5. Any amendment to or waiver of this Statement must be made in writing and signed by us.
6. You will not transfer any of your rights or obligations under this Statement to anyone else without our consent.

7. All of our rights and obligations under this Statement are freely assignable by us in connection with a merger, acquisition, or sale of assets, or by operation of law or otherwise.
8. Nothing in this Statement shall prevent us from complying with the law.
9. This Statement does not confer any third party beneficiary rights.
10. We reserve all rights not expressly granted to you.
11. You will comply with all applicable laws when using or accessing Facebook.

You may also want to review the following documents, which provide additional information about your use of Facebook:

- [Data Use Policy](#): The Data Use Policy contains information to help you understand how we collect and use information.
- [Payment Terms](#): These additional terms apply to all payments made on or through Facebook.
- [Platform Page](#): This page helps you better understand what happens when you add a third-party application or use Facebook Connect, including how they may access and use your data.
- [Facebook Platform Policies](#): These guidelines outline the policies that apply to applications, including Connect sites.
- [Advertising Guidelines](#): These guidelines outline the policies that apply to advertisements placed on Facebook.
- [Promotions Guidelines](#): These guidelines outline the policies that apply if you offer contests, sweepstakes, and other types of promotions on Facebook.
- [Facebook Brand Resources](#): These guidelines outline the policies that apply to use of Facebook trademarks, logos and screenshots.
- [How to Report Claims of Intellectual Property Infringement](#)
- [Pages Terms](#): These guidelines apply to your use of Facebook Pages.
- [Community Standards](#): These guidelines outline our expectations regarding the content you post to Facebook and your activity on Facebook.

To access the Statement of Rights and Responsibilities in several different languages, change the language setting for your Facebook session by clicking on the language link in the left corner of most pages. If the Statement is not available in the language you select, we will default to the English version.

From: Mithal, Maneesha </o=FTCEXCHANGE/ou=First Administrative Group/cn=Recipients/cn=MMITHAL>
Sent: Tuesday, November 12, 2013 9:11 AM
To: Olsen, Christopher <colsen@ftc.gov>; Berger, Laura <LBERGER@ftc.gov>
Subject: FW: Facebook Memo
Attach: facebook memo, NOvember 11 2013.docx

From: Rich, Jessica L.
Sent: Monday, November 11, 2013 2:09 PM
To: Kohn, James A.; Mithal, Maneesha
Cc: Kaufman, Daniel
Subject: RE: Facebook Memo

(b)(5)

From: Kohn, James A.
Sent: Friday, November 08, 2013 3:44 PM
To: Rich, Jessica L.; Mithal, Maneesha
Subject: FW: Facebook Memo

Duplicate

From: Kohm, James A. </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=JKOHM>
Sent: Wednesday, November 20, 2013 4:22 PM
To: Rich, Jessica L. <JRICH@ftc.gov>; Kaufman, Daniel <DKAUFMAN@ftc.gov>; Mithal, Maneesha <MMITHAL@ftc.gov>
Subject: FW: Facebook Memo20nov2013 - Copy.docx
Attach: 11.20.13.COMPARE.docx; Facebook Memo20nov2013 - Copy.docx

From: Rob Sherman <robsherman@fb.com>
Sent: Monday, October 21, 2013 5:30 PM
To: Mithal, Maneesha <MMITHAL@ftc.gov>; Olsen, Christopher <colsen@ftc.gov>
Cc: Erin Egan <erinegan@fb.com>; Edward Palmieri <ep@fb.com>
Subject: FW: Facebook Update

Maneesha and Chris,

We wanted to be sure that you'd seen the update below, which Ed sent to Laura and Reenah earlier today. Now that your team is back and hopefully things are starting to return to normal, Ed has suggested getting together with Laura and Reenah on Wednesday morning to talk through these points and some other things we'll be working on over the next few weeks. We'd be happy for you to join us (or to talk separately, if that's more convenient) if you'd like more information about any of this — just let us know.

Best,

Rob

Rob Sherman

Facebook | Manager, Privacy and Public Policy
1299 Pennsylvania Avenue, NW | Suite 800 | Washington, DC 20004
office 202.370.5147 | mobile 202.257.3901

From: Edward Palmieri <ep@fb.com>
Date: Monday, October 21, 2013 4:59 PM
To: "Koss, Laura" <LKOSS@ftc.gov>, "Kim, Reenah" <rkim1@ftc.gov>
Cc: Daniel Li <dli@fb.com>, Megan Alvarez <meganalvarez@fb.com>
Subject: Facebook Update

Dear Laura and Reenah,

Welcome back.

As part of our continuing efforts to maintain an open dialogue with you, we wanted to provide information on some recent developments. As you'll see, the first two updates are reminders of things we've already discussed and the third is an acquisition we announced last week. We're happy to discuss any or all of these with you at any time.

Additionally, we have a few other product updates coming in October that we'd be happy to come in and tell you about. If your schedule permits, perhaps we can schedule something for Wednesday morning? At your convenience, please let us know.

(b)(3):6(f),(b)(4)

(b)(3):21(f),(b)(4)

We are available to address any questions you may have and please do let us know if you are available for an in-person meeting on Wednesday AM to discuss some upcoming updates.

As always, thank you for you time.

Best,
Edward

edward palmieri | associate general counsel, privacy | facebook legal | ep@fb.com | 202.370.5154

From: Mithal, Maneesha </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=MMITHAL>
Sent: Monday, October 21, 2013 8:53 PM
To: Olsen, Christopher <colsen@ftc.gov>
Subject: Fw: Facebook Update

Can you attend?

Duplicate

From: Olsen, Christopher </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/
CN=RECIPIENTS/CN=COLSEN>
Sent: Wednesday, November 6, 2013 1:19 PM
To: Mithal, Maneesha <MMITHAL@ftc.gov>
Subject: FW: Fb
Attach: Commission memo (6nov2013 DRAFT).docx

(b)(5)

From: Berger, Laura
Sent: Wednesday, November 06, 2013 1:01 PM
To: Olsen, Christopher
Subject: FW: Fb

(b)(5)

From: Kim, Reenah
Sent: Wednesday, November 06, 2013 8:38 AM
To: Berger, Laura
Cc: Koss, Laura
Subject: Fb

Hi Laura,

(b)(5)

Thanks.
-Reenah

Reenah L. Kim
Federal Trade Commission
Bureau of Consumer Protection | Division of Enforcement
600 Pennsylvania Avenue NW | Mail Drop M-8102B | Washington, DC 20580
t:202.326.2272 | f:202.326.2558 | rkim1@ftc.gov

From: Rich, Jessica L. </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=JRICHT>
Sent: Wednesday, October 16, 2013 5:17 PM
To: Kohm, James A. <JKOHM@ftc.gov>; Mithal, Maneesha <MMITHAL@ftc.gov>
Subject: FW: NYT take on Facebook teen changes

(b)(5)

From: Jeffrey Chester
Sent: Wednesday, October 16, 2013 5:02 PM
To: Joy Spencer; Kathryn Montgomery; Jennifer Harris; Hudson
Subject: NYT take on Facebook teen changes

Facebook Changes Privacy Policy for Teenagers

By [VINDE GOEL](#)

Published: October 16, 2013

San Francisco — Teenagers using Facebook will now be able to post items that can be seen by the public, making it easier for the social network to turn a teenager's post into an ad that can be shown widely.

With the change to its rules on teenagers' use of Facebook, the company reversed its longstanding policy that users between 13 and 17 years old could not share comments and photos more broadly than to friends of friends.

Facebook said it made the change, announced on Wednesday, to let socially active teenagers like musicians and humanitarian activists, people the service has often called its "savviest users," reach a wider audience the way they can on blogs and rival services like Twitter.

But the move comes as Facebook tries to encourage its 1.2 billion users to share more information publicly. The company is locked in a battle with Twitter to convince advertisers that it is a better site for reaching consumers interested in events like sports, television shows and the news.

The Facebook move also comes as the [Federal Trade Commission conducts an inquiry](#) into other proposed changes to the company's privacy policies. Those policies would give Facebook automatic permission to take a user's post, including a post made by a teenager, and turn it into an advertisement broadcast to anyone who could have seen the original post.

Privacy advocates have complained to the F.T.C. that with those proposals, Facebook was violating a 2011 order that required the company to obtain explicit permission from its customers before using their data in advertising.

From: Jeffrey Chester </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=JEFFREYCHESTER>
Sent: Wednesday, October 16, 2013 10:31 AM
To: Mark Rotenberg <rotenberg@epic.org>; Hudson <hudson@democraticmedia.org>; Joy Spencer <joyspencer@democraticmedia.org>; Kathryn Montgomery <kcm@american.edu>; David Jacobs <jacobs@epic.org>
Subject: new FB data product, FYI

(b)(5)

From: Kohm, James A. </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=JKOHM>
Sent: Wednesday, November 13, 2013 3:11 PM
To: Rich, Jessica L. <JRICH@ftc.gov>; Kaufman, Daniel <DKAUFMAN@ftc.gov>; Mithal, Maneesha <MMITHAL@ftc.gov>
Subject: Proposed Statement for Tomorrow

(b)(5)

From: Mithal, Maneesha </o=FTCEXCHANGE/ou=First Administrative Group/cn=Recipients/cn=MMITHAL>
Sent: Thursday, November 14, 2013 1:19 PM
To: Kohm, James A. <JKOHM@ftc.gov>
Subject: q&a
Attach: qa2.docx

See my proposed additions in the attached.

From: Berger, Laura </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=LBERGER>
Sent: Tuesday, November 12, 2013 2:49 PM
To: Mithal, Maneesha <MMITHAL@ftc.gov>; Olsen, Christopher <colsen@ftc.gov>
Subject: RE: Cal AG collaboration

(b)(5)

From: Mithal, Maneesha
Sent: Tuesday, November 12, 2013 11:45 AM
To: Berger, Laura; Olsen, Christopher
Subject: Re: Cal AG collaboration

(b)(5)

From: Berger, Laura
Sent: Tuesday, November 12, 2013 02:43 PM
To: Mithal, Maneesha; Olsen, Christopher
Subject: RE: Cal AG collaboration

(b)(5)

From: Mithal, Maneesha
Sent: Tuesday, November 12, 2013 11:42 AM
To: Berger, Laura; Olsen, Christopher
Subject: Re: Cal AG collaboration

(b)(5)

From: Berger, Laura
Sent: Tuesday, November 12, 2013 02:36 PM
To: Mithal, Maneesha; Olsen, Christopher
Subject: RE: Cal AG collaboration

(b)(5)

(b)(5)

From: Mithal, Maneesha
Sent: Friday, November 08, 2013 6:34 PM
To: Berger, Laura; Olsen, Christopher
Subject: Re: Cal AG collaboration

(b)(5)

From: Berger, Laura
Sent: Friday, November 08, 2013 07:01 PM
To: Mithal, Maneesha; Olsen, Christopher
Subject: RE: Cal AG collaboration

(b)(5)

From: Berger, Laura
Sent: Friday, November 08, 2013 3:59 PM
To: Mithal, Maneesha; Olsen, Christopher
Subject: RE: Cal AG collaboration

(b)(5)

From: Mithal, Maneesha
Sent: Friday, November 08, 2013 3:53 PM
To: Berger, Laura; Olsen, Christopher
Subject: Fw: Cal AG collaboration

(b)(5)

From: Rich, Jessica L.
Sent: Friday, November 08, 2013 06:52 PM
To: Mithal, Maneesha
Subject: Re: Cal AG collaboration

(b)(5)

From: Mithal, Maneesha
Sent: Thursday, November 07, 2013 06:36 PM
To: Rich, Jessica L.
Subject: Fw: Cal AG collaboration

(b)(5)

From: Berger, Laura
Sent: Thursday, November 07, 2013 06:34 PM

To: Olsen, Christopher; Mithal, Maneesha
Subject: RE: Cal AG collaboration

(b)(5)

From: Berger, Laura
Sent: Thursday, November 07, 2013 9:22 AM
To: Olsen, Christopher; Mithal, Maneesha
Subject: RE: Cal AG collaboration

(b)(5)

From: Olsen, Christopher
Sent: Wednesday, November 06, 2013 7:01 PM
To: Berger, Laura; Mithal, Maneesha
Subject: Re: Cal AG collaboration

(b)(5)

From: Berger, Laura
Sent: Wednesday, November 06, 2013 07:15 PM
To: Mithal, Maneesha; Olsen, Christopher
Subject: RE: Cal AG collaboration

(b)(5)

From: Rich, Jessica L.
Sent: Wednesday, November 06, 2013 4:10 PM
To: Mithal, Maneesha; Kaufman, Daniel; Berger, Laura; Olsen, Christopher
Subject: Cal AG collaboration

(b)(5)

From: Rich, Jessica L.
Sent: Friday, November 01, 2013 08:32 AM
To: Mithal, Maneesha; Kaufman, Daniel; Berger, Laura
Subject: Fw: touching base

(b)(5)

From: Jeffrey Rabkin [<mailto:Jeffrey.Rabkin@doj.ca.gov>]
Sent: Friday, November 01, 2013 09:29 AM
To: Rich, Jessica L.
Subject: touching base

(b)(5)

From: Berger, Laura </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=LBERGER>
Sent: Friday, November 8, 2013 6:21 PM
To: Olsen, Christopher <colsen@ftc.gov>; Mithal, Maneesha <MMITHAL@ftc.gov>
Subject: RE: Cal AG collaboration

(b)(5)

From: Olsen, Christopher
Sent: Friday, November 08, 2013 3:13 PM
To: Mithal, Maneesha; Berger, Laura
Subject: Re: Cal AG collaboration

(b)(5)

From: Mithal, Maneesha
Sent: Friday, November 08, 2013 06:12 PM
To: Olsen, Christopher; Berger, Laura
Subject: Re: Cal AG collaboration

(b)(5)

From: Olsen, Christopher
Sent: Friday, November 08, 2013 06:10 PM
To: Berger, Laura; Mithal, Maneesha
Subject: Re: Cal AG collaboration

(b)(5)

From: Berger, Laura
Sent: Friday, November 08, 2013 06:08 PM
To: Olsen, Christopher; Mithal, Maneesha
Subject: RE: Cal AG collaboration

(b)(5)

From: Berger, Laura
Sent: Thursday, November 07, 2013 3:34 PM
To: Olsen, Christopher; Mithal, Maneesha
Subject: RE: Cal AG collaboration

(b)(5)

From: Berger, Laura
Sent: Thursday, November 07, 2013 9:22 AM
To: Olsen, Christopher; Mithal, Maneesha
Subject: RE: Cal AG collaboration

(b)(5)

(b)(5)

From: Olsen, Christopher
Sent: Wednesday, November 06, 2013 7:01 PM
To: Berger, Laura; Mithal, Maneesha
Subject: Re: Cal AG collaboration

(b)(5)

From: Berger, Laura
Sent: Wednesday, November 06, 2013 07:15 PM
To: Mithal, Maneesha; Olsen, Christopher
Subject: RE: Cal AG collaboration

(b)(5)

Duplicate

From: Olsen, Christopher </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=COLSEN>
Sent: Friday, November 8, 2013 6:13 PM
To: Mithal, Maneesha <MMITHAL@ftc.gov>; Berger, Laura <LBERGER@ftc.gov>
Subject: Re: Cal AG collaboration

(b)(5)

Duplicate

From: Olsen, Christopher </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=COLSEN>
Sent: Friday, November 8, 2013 6:12 PM
To: Berger, Laura <LBERGER@ftc.gov>; Mithal, Maneesha <MMITHAL@ftc.gov>
Subject: Re: Cal AG collaboration

(b)(5)

From: Berger, Laura
Sent: Friday, November 08, 2013 06:11 PM
To: Olsen, Christopher; Mithal, Maneesha
Subject: RE: Cal AG collaboration

(b)(5)

From: Olsen, Christopher
Sent: Friday, November 08, 2013 3:10 PM
To: Berger, Laura; Mithal, Maneesha
Subject: Re: Cal AG collaboration

(b)(5)

Duplicate

From: Mithal, Maneesha </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=MMITHAL>
Sent: Thursday, November 7, 2013 6:42 PM
To: Rich, Jessica L. <JRICH@ftc.gov>
Subject: Re: Cal AG collaboration

(b)(5)

From: Rich, Jessica L.
Sent: Thursday, November 07, 2013 06:41 PM
To: Mithal, Maneesha
Subject: Re: Cal AG collaboration

(b)(5)

From: Mithal, Maneesha
Sent: Thursday, November 07, 2013 06:36 PM
To: Rich, Jessica L.
Subject: Fw: Cal AG collaboration

(b)(5)

Duplicate

From: Berger, Laura </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=LBERGER>
Sent: Wednesday, November 6, 2013 7:16 PM
To: Mithal, Maneesha <MMITHAL@ftc.gov>; Olsen, Christopher <colsen@ftc.gov>
Subject: RE: Cal AG collaboration

(b)(5)

Duplicate

From: Olsen, Christopher </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=COLSEN>
Sent: Wednesday, October 23, 2013 2:33 PM
To: Mithal, Maneesha <MMITHAL@ftc.gov>
Subject: RE: did you see Asian American letter on Facebook privacy?

(b)(5)

From: Mithal, Maneesha
Sent: Monday, October 21, 2013 9:05 PM
To: Olsen, Christopher
Subject: did you see Asian American letter on Facebook privacy?

From: Olsen, Christopher </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=COLSEN>
Sent: Monday, October 21, 2013 10:43 PM
To: Mithal, Maneesha <MMITHAL@ftc.gov>
Subject: Re: did you see Asian American letter on Facebook privacy?

(b)(5)

From: Mithal, Maneesha
Sent: Monday, October 21, 2013 09:05 PM
To: Olsen, Christopher
Subject: did you see Asian American letter on Facebook privacy?

From: Olsen, Christopher </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=COLSEN>
Sent: Tuesday, November 5, 2013 12:29 PM
To: Mithal, Maneesha <MMITHAL@ftc.gov>
Subject: RE: Document1 [Compatibility Mode]

(b)(5)

From: Mithal, Maneesha
Sent: Tuesday, November 05, 2013 8:47 AM
To: Olsen, Christopher
Subject: Fw: Document1 [Compatibility Mode]

From: Kohm, James A.
Sent: Monday, November 04, 2013 12:05 PM
To: Mithal, Maneesha
Subject: Document1 [Compatibility Mode]

From: Mithal, Maneesha </o=FTCEXCHANGE/ou=First Administrative Group/cn=Recipients/cn=MMITHAL>
Sent: Monday, November 4, 2013 1:34 PM
To: Berger, Laura <LBERGER@ftc.gov>; Olsen, Christopher <colsen@ftc.gov>
Subject: RE: Facebook, financial lead-in, behavioral targeting (b)(5)

(b)(5)

From: Berger, Laura
Sent: Monday, November 04, 2013 12:30 PM
To: Mithal, Maneesha; Olsen, Christopher
Subject: RE: Facebook, financial lead-in, behavioral targeting (b)(5)

(b)(5)

From: Mithal, Maneesha
Sent: Monday, November 04, 2013 8:12 AM
To: Berger, Laura; Olsen, Christopher
Subject: FW: Facebook, financial lead-in, behavioral targeting (b)(5)

From: Jeffrey Chester
Sent: Monday, November 04, 2013 10:22 AM
To: Mithal, Maneesha
Subject: Facebook, financial lead-in, behavioral targeting (b)(5)

From: Berger, Laura </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=LBERGER>
Sent: Monday, November 4, 2013 1:54 PM
To: Mithal, Maneesha <MMITHAL@ftc.gov>; Olsen, Christopher <colsen@ftc.gov>
Subject: RE: Facebook, financial lead-in, behavioral targeting (b)(5)

(b)(5)

Duplicate

From: Rich, Jessica L. </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=JRICH>
Sent: Monday, October 21, 2013 8:01 AM
To: Jeffrey Chester <jeff@democraticmedia.org>; Mithal, Maneesha <MMITHAL@ftc.gov>; 'jkohn@ftc.gov'; Kohm, James A. <JKOHM@ftc.gov>
Cc: Hudson <hudson@democraticmedia.org>
Subject: Re: Facebook follow-up

Subbing Jim's correct email (it's kohm with an m). We received the materials, Jeff, and thank you and your team for them. Our staff will follow up if there are Qs. We are indeed behind but are very much back at work now.

Jessica L. Rich, Director
Bureau of Consumer Protection
Federal Trade Commission

From: Jeffrey Chester
Sent: Monday, October 21, 2013 07:47 AM
To: Rich, Jessica L.; Mithal, Maneesha; jkohn@ftc.gov <jkohn@ftc.gov>
Cc: Hudson
Subject: Facebook follow-up

Dear Jessica, Manesha and Jim:

I know you are just back to work, but just an FYI that we sent Jessica some follow-up materials, and are ready to provide additional information and analysis.

The market report, which I wrote, reflects just some of the data we have compiled on Fb's operations. I put in citations, but we have other material as well.

We hope the commission continues its review of Fb's proposed ToS/data plan, and ensures that its users--esp. teens--are protected by the consent decree.

Many thanks,

Jeff

Jeffrey Chester
Center for Digital Democracy
1621 Connecticut Ave, NW, Suite 550
Washington, DC 20009
www.democraticmedia.org
www.digitalads.org
202-986-2220

From: Olsen, Christopher </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=COLSEN>
Sent: Wednesday, November 6, 2013 8:46 AM
To: Mithal, Maneesha <MMITHAL@ftc.gov>
Subject: RE: Facebook meeting

Ok. I would like to.

-----Original Message-----

From: Mithal, Maneesha
Sent: Wednesday, November 06, 2013 7:56 AM
To: Olsen, Christopher
Subject: Facebook meeting

I made arrangements to go to the FB meeting. You're still welcome to come, but you don't have to.

From: Mithal, Maneesha </o=FTCEXCHANGE/ou=First Administrative Group/cn=Recipients/cn=MMITHAL>
Sent: Wednesday, November 6, 2013 8:52 AM
To: Olsen, Christopher <colsen@ftc.gov>
Subject: RE: Facebook meeting

Yes, excellent.

-----Original Message-----

From: Olsen, Christopher
Sent: Wednesday, November 06, 2013 8:46 AM
To: Mithal, Maneesha
Subject: RE: Facebook meeting

Ok. I would like to.

-----Original Message-----

From: Mithal, Maneesha
Sent: Wednesday, November 06, 2013 7:56 AM
To: Olsen, Christopher
Subject: Facebook meeting

I made arrangements to go to the FB meeting. You're still welcome to come, but you don't have to.

From: Mithal, Maneesha </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=MMITHAL>
Sent: Thursday, November 14, 2013 9:36 AM
To: Kim, Reenah <rkim1@ftc.gov>
Cc: Kohm, James A. <JKOHM@ftc.gov>; Koss, Laura <LKOSS@ftc.gov>; Kim, Laura <LKIM@ftc.gov>
Subject: RE: Facebook Memo 11-13.docx

(b)(5)

From: Kim, Reenah
Sent: Wednesday, November 13, 2013 6:06 PM
To: Mithal, Maneesha
Cc: Kohm, James A.
Subject: FW: Facebook Memo 11-13.docx

From: Kohm, James A.
Sent: Wednesday, November 13, 2013 6:04 PM
To: Rich, Jessica L.; Kaufman, Daniel
Cc: Mithal, Malini; Kim, Laura; Koss, Laura; Kim, Reenah
Subject: Facebook Memo 11-13.docx

From: Olsen, Christopher </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=COLSEN>
Sent: Tuesday, October 22, 2013 8:48 AM
To: 'Rob Sherman' <robsherman@fb.com>; Mithal, Maneesha <MMITHAL@ftc.gov>
Cc: Erin Egan <erinegan@fb.com>; Edward Palmieri <ep@fb.com>
Subject: RE: Facebook Update

Hi Rob. I am available to join your meeting Wednesday morning. Did you set a time and place yet?

From: Rob Sherman [mailto:robsherman@fb.com]
Sent: Monday, October 21, 2013 5:30 PM
To: Mithal, Maneesha; Olsen, Christopher
Cc: Erin Egan; Edward Palmieri
Subject: FW: Facebook Update

Maneesha and Chris,

We wanted to be sure that you'd seen the update below, which Ed sent to Laura and Reenah earlier today. Now that your team is back and hopefully things are starting to return to normal, Ed has suggested getting together with Laura and Reenah on Wednesday morning to talk through these points and some other things we'll be working on over the next few weeks. We'd be happy for you to join us (or to talk separately, if that's more convenient) if you'd like more information about any of this — just let us know.

Best,

Rob

Rob Sherman

Facebook | Manager, Privacy and Public Policy
1299 Pennsylvania Avenue, NW | Suite 800 | Washington, DC 20004
office 202.370.5147 | mobile 202.257.3901

From: Edward Palmieri <ep@fb.com>
Date: Monday, October 21, 2013 4:59 PM
To: "Koss, Laura" <LKOSS@ftc.gov>, "Kim, Reenah" <rkim1@ftc.gov>
Cc: Daniel Li <dli@fb.com>, Megan Alvarez <meganalvarez@fb.com>
Subject: Facebook Update

Dear Laura and Reenah,

Welcome back.

As part of our continuing efforts to maintain an open dialogue with you, we wanted to provide information on some recent developments. As you'll see, the first two updates are reminders of things we've already discussed and the third is an acquisition we announced last week. We're happy to discuss any or all of these with you at any time.

Additionally, we have a few other product updates coming in October that we'd be happy to come in and tell you about. If your schedule permits, perhaps we can schedule something for Wednesday morning? At your convenience, please let us know.

Facebook Updates

1. Who can look up your timeline by name?

Per our announcement to users last December (which we shared with you then and again a few weeks ago), we are retiring a legacy setting called “Who can look up your Timeline by name?” As we explained, this setting only controlled whether someone could be found when people typed their name into the Facebook search bar. The setting was created when Facebook was a simple directory of profiles and was very limited in applicability. For example, it didn’t prevent people from navigating to a person’s Timeline by clicking on that person’s name in News Feed stories or from a mutual friend’s Timeline, or from conducting other searches where they may be included in the results.

Our goal is to help Facebook users understand that the best way to control what others can see about them is to choose who can see the individual things they share. Starting approximately a week ago, if someone is still using the old setting, they will see a notice on their homepage and be directed to tools and further information on how to control their information on Facebook. These tools provide a range of controls, including the ability to change the audience of the things that have been posted and to delete old posts that users wish to remove. We will not make a change until these users have clicked to accept the notice.

2. Changes to teenagers’ post audiences

We are implementing a few changes to the way teenagers post on Facebook. As you’ll recall, our plan is to give teenagers the option to post publicly—as they can on most other websites—but to narrow the default audience for their posts from “Friends of Friends” to “Friends.” We’ll also add significant in-product education to make it obvious when teenagers choose to post publicly. We’ve engaged in significant external consultations on these changes and believe these are positive changes for teens.

3. Onavo Acquisition

On October 14th, Facebook announced its intention to acquire Onavo, Inc. Onavo offers mobile utility apps that help consumers save money by allowing them to understand and reduce their mobile data usage. For example, after a user installs Onavo’s flagship Extend app, the app connects the mobile device to Internet services through Onavo’s systems, thereby allowing Onavo to analyze, compress, and make more efficient the device’s access to data services. By holistically compressing mobile data, Extend allows people to access websites and enjoy apps as they always have, but without using as much data—so their mobile charges are reduced. And, by providing users with a breakdown of their data usage, users can see how much data is being consumed by the things they do from their device and make informed data usage choices. Facebook believes these capabilities will be extremely valuable to the critical goal of Internet.org by improving the efficiency of mobile data usage and allowing more people around the world to connect and share.

* * *

We are available to address any questions you may have and please do let us know if you are available for an in-person meeting on Wednesday AM to discuss some upcoming updates.

As always, thank you for you time.

Best,
Edward

From: Olsen, Christopher </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=COLSEN>
Sent: Monday, October 21, 2013 10:42 PM
To: Mithal, Maneesha <MMITHAL@ftc.gov>
Subject: Re: Facebook Update

Yes

From: Mithal, Maneesha
Sent: Monday, October 21, 2013 08:53 PM
To: Olsen, Christopher
Subject: Fw: Facebook Update

Can you attend?

Duplicate

From: Rob Sherman <robsherman@fb.com>
Sent: Tuesday, October 22, 2013 4:14 PM
To: Olsen, Christopher <colsen@ftc.gov>; Mithal, Maneesha <MMITHAL@ftc.gov>
Cc: Erin Egan <erinegan@fb.com>; Edward Palmieri <ep@fb.com>
Subject: Re: Facebook Update

Hi Chris,

Laura and Reenah proposed 11:00 at 1800 M. Does that work for you?

Thanks.

Rob

Duplicate

From: Olsen, Christopher </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=COLSEN>
Sent: Wednesday, November 6, 2013 1:33 PM
To: Mithal, Maneesha <MMITHAL@ftc.gov>
Subject: RE: Fb

(b)(5)

From: Mithal, Maneesha
Sent: Wednesday, November 06, 2013 1:27 PM
To: Olsen, Christopher
Subject: RE: Fb

(b)(5)

From: Olsen, Christopher
Sent: Wednesday, November 06, 2013 1:19 PM
To: Mithal, Maneesha
Subject: FW: Fb

(b)(5)

From: Berger, Laura
Sent: Wednesday, November 06, 2013 1:01 PM
To: Olsen, Christopher
Subject: FW: Fb

(b)(5)

From: Kim, Reenah
Sent: Wednesday, November 06, 2013 8:38 AM
To: Berger, Laura
Cc: Koss, Laura
Subject: Fb

Hi Laura,

(b)(5)

Thanks,
-Reenah

Reenah L. Kim
Federal Trade Commission
Bureau of Consumer Protection | Division of Enforcement
600 Pennsylvania Avenue NW | Mail Drop M-8102B | Washington, DC 20580
t:202.326.2272 | f:202.326.2558 | rkim1@ftc.gov

From: Berger, Laura </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=LBERGER>
Sent: Thursday, November 14, 2013 8:54 PM
To: Mithal, Maneesha <MMITHAL@ftc.gov>; Olsen, Christopher <colsen@ftc.gov>
Subject: Re: Fb meeting

Great, (b)(6) (b)(5) Thanks.

----- Original Message -----

From: Mithal, Maneesha
Sent: Thursday, November 14, 2013 06:47 PM
To: Berger, Laura; Olsen, Christopher
Subject: Fb meeting

(b)(5)

From: Olsen, Christopher </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=COLSEN>
Sent: Thursday, November 14, 2013 7:20 PM
To: Mithal, Maneesha <MMITHAL@ftc.gov>
Subject: Re: Fb meeting

Ah. I remember you mentioned this but I never got a scheduler. Maybe there wasn't one...

----- Original Message -----

From: Mithal, Maneesha
Sent: Thursday, November 14, 2013 07:18 PM
To: Olsen, Christopher
Subject: Re: Fb meeting

It's tomorrow at 9.30. (b)(5)

----- Original Message -----

From: Olsen, Christopher
Sent: Thursday, November 14, 2013 07:14 PM
To: Mithal, Maneesha
Subject: Re: Fb meeting

(b)(5)

Duplicate

From: Olsen, Christopher </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=COLSEN>
Sent: Wednesday, November 6, 2013 5:08 PM
To: Mithal, Maneesha <MMITHAL@ftc.gov>
Subject: Re: FB meeting

Are you meeting with edith at 5?

From: Mithal, Maneesha
Sent: Wednesday, November 06, 2013 04:56 PM
To: Olsen, Christopher
Subject: Re: FB meeting

I'm here already - JB moved our meeting to 5. You can park in HQ garage after 5, I think.

Duplicate

From: Olsen, Christopher </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=COLSEN>
Sent: Wednesday, November 6, 2013 4:56 PM
To: Mithal, Maneesha <MMITHAL@ftc.gov>
Subject: RE: FB meeting

ok

Duplicate

From: Berger, Laura </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=LBERGER>
Sent: Friday, November 15, 2013 9:35 AM
To: Mithal, Maneesha <MMITHAL@ftc.gov>
Subject: Re: Fb meeting

You waiting on FB?

(b)(6)

Duplicate

From: Mithal, Maneesha </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=MMITHAL>
Sent: Wednesday, November 6, 2013 1:33 PM
To: Olsen, Christopher <colsen@ftc.gov>
Subject: RE: Fb

I'm in HQ, and I'll try to link up with Jim on this.

From: Olsen, Christopher
Sent: Wednesday, November 06, 2013 1:33 PM
To: Mithal, Maneesha
Subject: RE: Fb

(b)(5)

Duplicate

From: Rich, Jessica L. </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=JRICH>
Sent: Tuesday, October 15, 2013 10:29 AM
To: Jeffrey Chester <jeff@democraticmedia.org>; Mithal, Maneesha <MMITHAL@ftc.gov>; Kohm, James A. <JKOHM@ftc.gov>; Koss, Laura <LKOSS@ftc.gov>; Wolfe, Douglas <DWOLFE@ftc.gov>; Kim, Reenah <rkim1@ftc.gov>; Poss, Patricia H. <PPOSS@ftc.gov>; Hasty, Andrew <ahasty@ftc.gov>; Berger, Laura <LBERGER@ftc.gov>
Cc: Hudson <hudson@democraticmedia.org>; Joy Spencer <joyspencer@democraticmedia.org>
Subject: RE: followup docs, Facebook ToS

Thanks Jeff. We can't review this now but will definitely take a close look when we return to work -- hopefully very, very soon.

From: Jeffrey Chester
Sent: Tuesday, October 15, 2013 10:19 AM
To: Rich, Jessica L.; Mithal, Maneesha; Kohm, James A.; Koss, Laura; Wolfe, Douglas; Kim, Reenah; Poss, Patricia H.; Hasty, Andrew; Berger, Laura
Cc: Hudson; Joy Spencer
Subject: followup docs, Facebook ToS

Dear FTC staff:

Needless to say, I hope the commission and the gov't returns to work soon.

At our meeting, we promised to send follow-up information. Attached are two docs from CDD--a legal memo and one on Facebook's marketing practices and data collection.

We will contact you after you reopen to discuss a meeting on these issues. Of course, we are happy to provide you with any additional information that could be of assistance.

Many thanks,

Jeff

PS: I do want to also draw your attention to the role of financial data involved with Facebook's data collection/targeting enabled marketing practices (cited in our market analysis). Indeed, due to my research on financial marketing, for a forthcoming report, I was served a payday ad loan on Facebook (delivered via one of Fb's exchange partners). Financial data involves both sensitive information and the need for consumer safeguards. Given the FTC's concern about new financial marketing practices, it is an area that the commission should also focus on as part of its Fb review. We also, of course, believe that adolescents require the same sensitive data safeguards.

Jeffrey Chester
Center for Digital Democracy
1621 Connecticut Ave, NW, Suite 550
Washington, DC 20009
www.democraticmedia.org
www.digitalads.org
202-986-2220

From: Kohm, James A. </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=JKOHM>
Sent: Thursday, November 14, 2013 10:31 AM
To: Rich, Jessica L. <JRICH@ftc.gov>; Kaplan, Peter P. <pkaplan@ftc.gov>; Mayfield III, Jay <jmayfield@ftc.gov>; Mithal, Maneesha <MMITHAL@ftc.gov>
Cc: Kaufman, Daniel <DKAUFMAN@ftc.gov>
Subject: RE: for friday

I'll send around a draft this afternoon.

From: Rich, Jessica L.
Sent: Wednesday, November 13, 2013 6:11 PM
To: Kaplan, Peter P.; Mayfield III, Jay; Kohm, James A.; Mithal, Maneesha
Cc: Kaufman, Daniel
Subject: Fw: for friday

(b)(5)

Jessica L. Rich, Director
Bureau of Consumer Protection
Federal Trade Commission

From: Hipsley, Heather
Sent: Wednesday, November 13, 2013 06:03 PM
To: Rich, Jessica L.; Kestenbaum, Janis
Subject: for friday

(b)(5)

From: Kohm, James A. </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=JKOHM>
Sent: Thursday, November 14, 2013 3:56 PM
To: Rich, Jessica L. <JRICH@ftc.gov>; Kaplan, Peter P. <pkaplan@ftc.gov>; Mayfield III, Jay <jmayfield@ftc.gov>; Mithal, Maneesha <MMITHAL@ftc.gov>
Cc: Kaufman, Daniel <DKAUFMAN@ftc.gov>
Subject: RE: for friday
Attach: Facebook Q & A.docx

Draft Attached

Duplicate

From: Mithal, Maneesha </o=FTCEXCHANGE/ou=First Administrative Group/cn=Recipients/cn=MMITHAL>
Sent: Monday, November 4, 2013 2:48 PM
To: Kaufman, Daniel <DKAUFMAN@ftc.gov>; Kohm, James A. <JKOHM@ftc.gov>
Cc: Rich, Jessica L. <JRICHT@ftc.gov>
Subject: RE: Markey

(b)(5)

From: Kaufman, Daniel
Sent: Monday, November 04, 2013 2:47 PM
To: Kohm, James A.; Mithal, Maneesha
Cc: Rich, Jessica L.
Subject: Markey

(b)(5)

From: Mithal, Maneesha </o=FTCEXCHANGE/ou=First Administrative Group/cn=Recipients/cn=MMITHAL>
Sent: Wednesday, November 13, 2013 4:01 PM
To: Kohm, James A. <JKOHM@ftc.gov>; Rich, Jessica L. <JRICH@ftc.gov>; Kaufman, Daniel <DKAUFMAN@ftc.gov>
Subject: RE: Proposed Statement for Tomorrow

(b)(5)

From: Kohm, James A.
Sent: Wednesday, November 13, 2013 3:11 PM
To: Rich, Jessica L.; Kaufman, Daniel; Mithal, Maneesha
Subject: Proposed Statement for Tomorrow

(b)(5)

From: Kohm, James A. </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=JKOHM>
Sent: Monday, November 18, 2013 12:50 PM
To: Rich, Jessica L. <JRICH@ftc.gov>; Kaufman, Daniel <DKAUFMAN@ftc.gov>; Mithal, Maneesha <MMITHAL@ftc.gov>
Subject: RE: Revised Memo Based on Friday's Meeting

(b)(5)

From: Rich, Jessica L.
Sent: Monday, November 18, 2013 12:49 PM
To: Kohm, James A.; Kaufman, Daniel; Mithal, Maneesha
Subject: RE: Revised Memo Based on Friday's Meeting

(b)(5)

From: Kohm, James A.
Sent: Monday, November 18, 2013 12:48 PM
To: Rich, Jessica L.; Kaufman, Daniel; Mithal, Maneesha
Subject: Revised Memo Based on Friday's Meeting

From: Mithal, Maneesha </o=FTCEXCHANGE/ou=First Administrative Group/cn=Recipients/cn=MMITHAL>
Sent: Thursday, November 14, 2013 2:29 PM
To: Olsen, Christopher <colsen@ftc.gov>
Cc: Berger, Laura <LBERGER@ftc.gov>
Subject: RE: Should we call CA ag's office re FB or did you want to do that?

(b)(5)

From: Olsen, Christopher
Sent: Thursday, November 14, 2013 1:45 PM
To: Mithal, Maneesha
Subject: FW: Should we call CA ag's office re FB or did you want to do that?

(b)(5)

From: Berger, Laura
Sent: Thursday, November 14, 2013 1:31 PM
To: Olsen, Christopher
Subject: Re: Should we call CA ag's office re FB or did you want to do that?

(b)(5)

From: Olsen, Christopher
Sent: Thursday, November 14, 2013 01:28 PM
To: Berger, Laura
Subject: RE: Should we call CA ag's office re FB or did you want to do that?

(b)(5)

From: Berger, Laura
Sent: Thursday, November 14, 2013 12:42 PM
To: Olsen, Christopher
Subject: Re: Should we call CA ag's office re FB or did you want to do that?

(b)(5)

From: Olsen, Christopher
Sent: Thursday, November 14, 2013 08:56 AM
To: Berger, Laura
Subject: FW: Should we call CA ag's office re FB or did you want to do that?

fyi

From: Mithal, Maneesha
Sent: Thursday, November 14, 2013 8:03 AM
To: Rich, Jessica L.
Cc: Olsen, Christopher
Subject: Re: Should we call CA ag's office re FB or did you want to do that?

(b)(5)

From: Rich, Jessica L.
Sent: Thursday, November 14, 2013 07:48 AM
To: Mithal, Maneesha
Subject: RE: Should we call CA ag's office re FB or did you want to do that?

(b)(5)

From: Mithal, Maneesha
Sent: Thursday, November 14, 2013 7:25 AM
To: Rich, Jessica L.
Subject: Should we call CA ag's office re FB or did you want to do that?

From: Berger, Laura </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=LBERGER>
Sent: Thursday, November 14, 2013 4:28 PM
To: Mithal, Maneesha <MMITHAL@ftc.gov>; Olsen, Christopher <colsen@ftc.gov>
Subject: Re: Should we call CA ag's office re FB or did you want to do that?

(b)(5)

Duplicate

From: Kohm, James A. </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=JKOHM>
Sent: Monday, November 18, 2013 12:48 PM
To: Rich, Jessica L. <JRICH@ftc.gov>; Kaufman, Daniel <DKAUFMAN@ftc.gov>; Mithal, Maneesha <MMITHAL@ftc.gov>
Subject: Revised Memo Based on Friday's Meeting
Attach: Facebook Mem18nov2013.docx

From: Berger, Laura </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=LBERGER>
Sent: Friday, November 15, 2013 11:10 AM
To: Rich, Jessica L. <JRICH@ftc.gov>; Olsen, Christopher <colsen@ftc.gov>; Mithal, Maneesha <MMITHAL@ftc.gov>; Kohm, James A. <JKOHM@ftc.gov>
Subject: Today's FB Meeting

(b)(5)

Laura

From: Olsen, Christopher </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=COLSEN>
Sent: Thursday, October 24, 2013 2:59 PM
To: Mithal, Maneesha <MMITHAL@ftc.gov>
Subject: we need to discuss facebook

Christopher N. Olsen
Assistant Director
Division of Privacy and Identity Protection
Federal Trade Commission
601 New Jersey Ave., NW
Mail Stop NJ-8122
Washington, DC 20001
tel. 202 326-3621
fax 202 326-3768