



July 26, 2013

VIA EMAIL AND FEDERAL EXPRESS

Reenah L. Kim
Laura D. Koss
Division of Enforcement
Federal Trade Commission
Washington, DC 20580

Re: *In the Matter of Facebook, Inc.*, Docket No. C-4365

Dear Reenah and Laura,

Enclosed please find additional materials relating to the comprehensive assessment and report (“Assessment”) prepared by PricewaterhouseCoopers (the “Independent Assessor”) and provided to you on April 22, 2013, pursuant to Part V of the Decision and Order entered in *In re Facebook*, Docket No. C-4365 (July 27, 2012) (“Order”). In accordance with Part V, the Assessment examined the sufficiency of Facebook’s Privacy Program during the period from August 15, 2012 to February 11, 2013. We are proud that the Independent Assessor concluded that Facebook’s Privacy Program was operating effectively throughout the reporting period and believe that the comprehensive report—which details the extensive and rigorous testing performed by PricewaterhouseCoopers—speaks for itself. Nonetheless, to further our open and constructive dialogue with you, we have provided additional information herein to help facilitate your review of the Assessment.

Please note that material contained in this response constitutes Facebook’s confidential business information and should be treated with the highest degree of confidentiality pursuant to 5 U.S.C. §§ 552(b)(3) & (b)(4) and 15 U.S.C. § 46(f).

Privacy Assessment

Privacy is central to everything we do at Facebook. We have worked systematically to develop practices and procedures to secure users’ personal information and share that information in accordance with their settings and choices. In line with these goals, Facebook has collaborated with the FTC and the Office of the Data Protection Commissioner in Ireland to produce thorough reviews of our compliance with our privacy and data protection obligations. These reviews are comprehensive and document Facebook’s privacy controls, describe the testing

procedures used to assess whether the controls were operating effectively, address and rebut a number of misperceptions about how Facebook approaches privacy, and identify areas where we can continue to improve.

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

Deletion and Third-Party Access

For both Instagram and Facebook, you asked us to clarify our compliance with Section III of the Order, which states: “[Respondent shall] 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” Facebook and Instagram are in compliance with this obligation—when users delete their photos or videos on Instagram, or the things they post on Facebook, such content is disabled almost immediately and no longer accessible through the services.

Separately, as you have noted, our Assessment reported that when Facebook accounts are deleted, we run processes to delete the account and the content associated with it. This account deletion process goes beyond our commitment in Section III of the Order. (b)(4);

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

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

For

additional information on the Independent Assessor’s testing and review of Facebook’s account deletion processes, please see page 45 of the Assessment.



Non-user Information

You asked us about information we receive and store about non-users. The vast majority of information Facebook receives is through the services we provide to users that have registered with us. As part of the tools and services we offer, we sometimes receive information about non-users. The most common example is when users import their contacts to Facebook so they can find friends to connect with. These imported contacts may include information about non-users, who can be invited by the user to join Facebook. We store and use the imported contacts on behalf of the user who imported them to provide our tools and services. The contacts are kept until the user deletes the information, which they can do at any time.

Product Review, Risk Assessment, and Supplemental Materials

You asked for more information about the product review and risk assessment elements of our Privacy Program and for other supplemental materials, such as related policies and procedures. Because of confidentiality and privilege concerns, we are not able to provide you with certain information about the privacy-related decisions discussed in our product review sessions or share copies of our internal risk assessment. However, we have included below additional information about our product review program and our risk assessment process, and have attached a range of supplemental documents for your review. We hope these materials are helpful and provide additional context for the Assessment.

Product Review

Facebook designed its product review process to facilitate privacy reviews at the earliest stages in the product development process. (b)(4); (b)(3):6(f)

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



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

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

For additional information on the Independent Assessor's testing and review of Facebook's product review process, please see pages 34, 35 and 44 of the Assessment.

During the Assessment period, the XFN reviewed approximately 300 products or features. As part of our supplemental documents, we have included a redacted example of the materials created for the Privacy Cross-Functional Team to facilitate the review process described above (see Exhibit A).

Risk Assessment

A subgroup of the Privacy Cross-Functional Team, also known as "Privacy Governance Team" or "Core XFN," has worked to evaluate Facebook's privacy risks. That review resulted in a privacy risk assessment and an ongoing process aimed at identifying reasonably foreseeable, material risks, both internal and external. Discussions related to the risk assessment involve, among others, representatives from Privacy, Engineering, Security, Internal Audit, Legal, Policy, Finance, Platform Operations, and User Operations, and consider risks in each relevant area of operation, including governance, product design and engineering (including product development and research), user operations, advertising, service providers, employee training and management (including training on the requirements of the Order), and security.

In addition, Facebook performs a systematic and collaborative review of its risk assessment during its annual "Privacy Summit," which includes a broader group of stakeholders from the Privacy Cross-Functional Team. Attendees of the annual Privacy Summit review, discuss, and update the risk assessment in light of changing internal and external risks, changes in operations, and changes in laws and regulations. The sufficiency of existing controls in mitigating identified risks (as well as expected future risks) is also evaluated.

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

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

For additional information on the Independent Assessor's testing and review of Facebook's risk assessment, please see pages 24 and 74 of the Assessment.

Supplemental Materials

We have enclosed a representative collection of core documents related to Facebook's privacy program. These include:

- **Facebook Privacy Process Overview:** This document provides an introduction to Facebook's privacy review process and includes overviews of the Privacy-PM team, Privacy Training, and the Privacy Cross Functional Review process (*see* Exhibit B).
- **Personnel Relevant to Privacy Program/Privacy Controls:** This document contains a list of those involved in the development and implementation of Facebook's privacy program, identified by job title and department (*see* Exhibit C).
- **Data Sharing Standards:** This document clarifies how to categorize Facebook data and how to handle such data (*see* Exhibit D).
- **Code of Conduct:** This document outlines the Facebook employee Code of Conduct and discusses requirements around the protection of user data (*see* Exhibit E).
- **Facebook User Information Access Agreement:** This agreement outlines the obligations of Facebook employees with respect to Facebook User Information (information relating to users of Facebook unavailable to the general public) (*see* Exhibit F).
- **Confidential Information and Invention Assignment Agreement for U.S. Employees (California):** This agreement outlines the conditions of employment at Facebook (*see* Exhibit G).
- **Information Security Policy:** This document provides guidance on preventing the unwanted disclosure, modification, or destruction of Facebook information (*see* Exhibit H).
- **Facebook Vendor Security/Web Application Security Review:** This document includes information regarding Facebook's vendor security review process, including vendor security assessments and the application process (*see* Exhibit I).
- **Standard Contract Language:** This document shows representative data provisions from our template Professional Services Agreement (*see* Exhibit J).
- **Data Use Policy:** This document describes the data that Facebook receives and how it is used and shared (*see* Exhibit K).
- **Statement of Rights and Responsibilities:** This document provides our terms of service, which governs our relationship with users and others who interact with Facebook (*see* Exhibit L).
- **Facebook Platform Policies:** This document addresses the obligations that must be



followed by Platform applications and developers and includes provisions related to the storage/usage of data provided by Facebook (see Exhibit M).

* * *

We hope that you find the additional information helpful and informative to your review of the Assessment. Please do not hesitate to contact us should you have any additional questions.

Kind regards,

A handwritten signature in black ink, appearing to read 'E. Palmieri', is positioned below the text 'Kind regards,'.

Edward Palmieri
Associate General Counsel, Privacy
Facebook, Inc.
1155 F. Street, NW Suite 475
Washington, DC 20004

Exhibit A

Discussions

- | | |
|---|---|
| 1 | Cable: Subscribe for Pages |
| 2 | Tag Anyone in Groups |
| 3 | Skills |
| 4 | Profile Completeness |
| 5 | SDK Terms Change |
| 6 | Unity Internal Use and Targeting Cluster |
| 7 | Mobile Links to Privacy Settings and Terms Update |
| 8 | Instagram Privacy Policy Update |
| 9 | Heads Up: QR Code Friending |

Other Updates

- 1 [REDACTED] for Pages
- 2 Auto Shut-off for Notifications
- 3 Self-Serve Frequency Capping
- 4 Pages Manager v1.6
- 5 Mobile on IO
- 6 [REDACTED] Thread Merge and Contact Sync

Updates Sent Earlier this week

- 1 Updates to the Privacy Settings Page [REDACTED]
- 2 [REDACTED] 1.1.1
- 3 Editing M-Touch Profile Info

Discussions

Cable: Subscribe for Pages

Cable: Subscribe for Pages

- What it is:
 - Allow users to subscribe to Pages
 - Tentative Launch: [REDACTED]
- Privacy Issues:
 - [REDACTED]
 - [REDACTED]

Cable: Subscribe for Pages

- Privacy Decisions:

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

Tag Anyone in Groups, Events & Messages

Tag Anyone in Groups, Events, Messages

- What it is:

- Tag anyone in groups

- Privacy Issues / Decisions:

- [REDACTED]
 - [REDACTED]
 - [REDACTED]

Skills

Skills

- **What it is:**
 - Allow users to enter professional skills in their About tab on Timeline
 - Skills are linked to wikipedia community “hub” pages
- **Privacy Issues:**
 - [REDACTED]
- **Privacy Decisions:**
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]

Profile Completeness

Profile Completeness

- What it is:
 - Prompt users to enter empty profile fields for location, work and education
- Privacy Issues / Decisions:
 - [REDACTED]
 - [REDACTED]

SDK ToS Change

SDK ToS Change

- What it is:
 - Add language to SDK ToS to require affirmation that the site has provided notice to its users that their site uses third-party measurement
- Privacy Issues / Decisions:
 - [REDACTED]
 - [REDACTED]

Unity Data Use and Targeting Cluster

Unity Data Use and Targeting Cluster

- What it is:
 - We know which users have the unity plugin installed.
- Privacy Issues

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

Unity Data Use and Targeting Cluster

- Decisions:

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

Mobile Links to Privacy Settings and Terms Update

Mobile Links to Privacy Settings and Terms Update

- What it is:

- Update to left nav links to Privacy Settings and Terms and Policies.

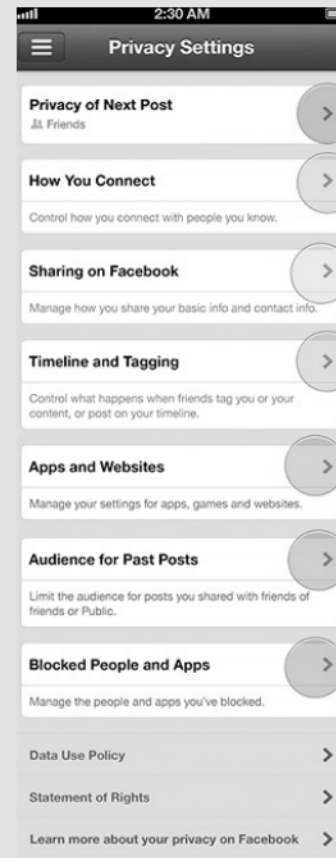
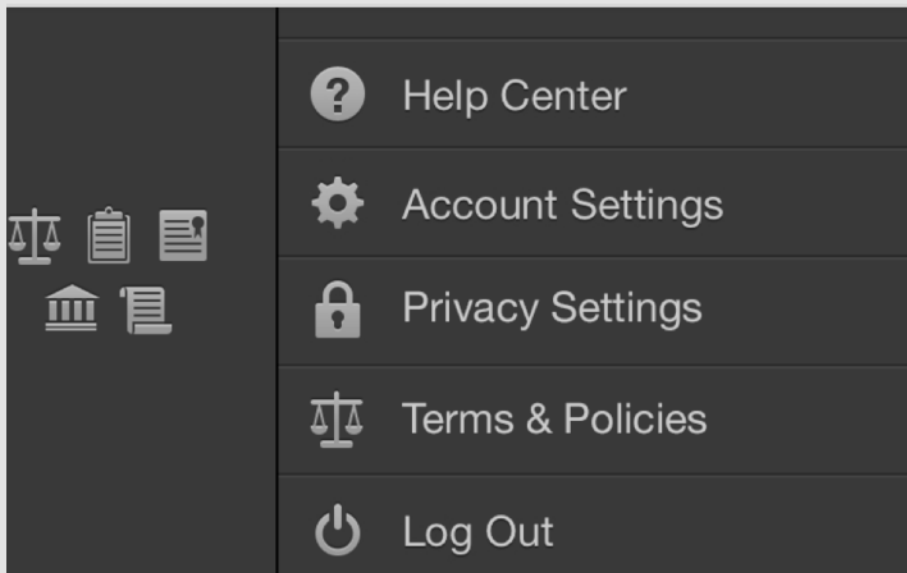
- Issues:

- [REDACTED]

Decisions:

- [REDACTED]
- [REDACTED]
- [REDACTED]

Mobile Links to Privacy Settings and Terms Update



Instagram Privacy Policy Update

Heads Up: QR Code Friending

QR Code Friending

- What it is:
 - Scan a QR code to be taken to a user's timeline (and add them as friend)
 - Currently available on feature phones in Japan, rolling out on smartphones by EOY
 - V2 (still in development): scanning QR code would auto-friend the person

- Privacy Issues / Decisions:

- [REDACTED]
- [REDACTED]

Other Updates



[REDACTED] for Pages

[REDACTED] for Pages

- **What it is:**

- Allow users to opt-in to receiving notifications about a Page's activity
- Tentative launch: [REDACTED]

- **Privacy Issues/Decisions:**

- [REDACTED]

Auto-Shutoff for Notifications

Auto-Shutoff for Notifications

- What it is:
 - Auto-detect users who have gone stale or are not interacting with certain app notifications and turn off those notifications
 - Tentative launch: [REDACTED]
- Privacy Issues/Decisions:
 - [REDACTED]
 - [REDACTED]

Self-Serve Frequency Capping

Self-Serve Frequency Capping

- What it is:
 - Allow advertisers to set daily frequency caps on their ads
 - Launch timing still TBD
- Privacy Issues/Decisions:
 - [REDACTED]

Pages Manager v16

Pages Manager v1.6

- What it is:
 - Pages manager's next iPhone version – supports iPhone 5 and bug fixes
- Privacy Issues / Decisions:
 - 

Mobile on IO

Mobile on IO

- What it is:
 - Offering guarantees on mobile
 - Tentative launch [REDACTED]
- Privacy Issues / Decisions:
 - [REDACTED]



Thread Merging and Contact Syncing

[REDACTED] Thread Merging and Contact Syncing

What is it: [REDACTED] is the next release of messenger for android. Users can both SMS message and FB message other users through the app.

- Launch Date: [REDACTED] (tentative)

- Issue: [REDACTED]

[REDACTED] Thread Merging and Contact Syncing

- Issues/Decisions:

- [REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
- [REDACTED]

Previous Updates Sent This Week

Updates to Privacy Settings Page



Updates to Privacy Settings Page

- What it is:
 - Updates to privacy settings page
- Privacy Decisions:

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

[REDACTED] 1.1.1 (sent [REDACTED])

[REDACTED] 1.1.1

- **What it is:** : Update to the iOS camera app that includes bug fixes and a change for device permissions flows.

- **Issue:** [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

- **Decision:**
[REDACTED]
[REDACTED]

1.1.1



Editing M Touch Profile Info (sent)

Editing M Touch Profile Info

- **What it is:** Mobile profile editing issues are a top support issue, particularly on m-touch. For m-touch users, the identity team is rolling out the ability to edit (both change and add) the family and relationship fields.

- **Issue:** [REDACTED]
[REDACTED]

- **Decisions:**

- [REDACTED]
[REDACTED]
[REDACTED]

- [REDACTED]
[REDACTED]

Exhibit B

1. Introduction.

As a company, Facebook encourages its product teams to “Move Fast” and “Be Bold.” Facebook encourages change as often as necessary.

The Privacy PM team supports speed of development, and products by serving as a centralized resource to identify and resolve privacy, policy, security, performance, legal, or integrity issues.

The team prioritizes solutions. Privacy PMs may, for example, advise product managers, research an issue for a product manager, or set up meetings between product teams and other involved parties. The team's value is in preventing problems, speeding up the build process, and advocating privacy across teams.

The Facebook Privacy Review Process is designed to ensure the consideration of privacy impact to users when designing new products and updating existing features (“Privacy by Design”).

This Review Process attempts to achieve the following core processes:

- Establish a team dedicated to: (1) providing guidance to product teams on privacy design questions; (2) coordinating feedback from privacy stakeholders; and (3) driving resolution of privacy issues
- Educate Engineers, Product Managers, Content Strategists, Product Marketing Managers, and others on the existing Facebook privacy framework and legal obligations to users
- Hold weekly cross-functional reviews of key privacy decisions and material changes to the privacy framework with key stakeholders across Facebook (“Privacy XFN”).
- Provide guidance and support on bug resolution where user privacy is impacted
- Ensure consistent decision making on privacy issues across Facebook

2. The Privacy Program Management Team.

The Privacy Review Process is driven by the Privacy Program Management Team. It is led by the Chief Privacy Officer of Product and is staffed with dedicated program managers (“Privacy PM’s”) who align with specific product verticals.

Among other things, the Privacy PM team is responsible for:

- **Conducting Privacy Training Sessions.** Monthly and as requested, described in detail in section 3, “Privacy Training”
- **Holding Open Office Hours.** Office hours are held once a week. Anyone can schedule time or just drop in to meet with the Privacy PMs. Engineers and Product Managers often use this time to get initial feedback on products or new features they are starting to build.

Privacy Process Overview

- **Coordinating Meetings (pre-cross functional review).** In many instances, the Privacy PM team coordinates meetings with legal, policy, product marketing, content strategy or other product teams. These generally are pre-cursors to the XFN Review of a product.
- **Coordinating the weekly Privacy Cross Functional Review.** The Privacy PM team is responsible for the scheduling, preparation, management and documentation of the weekly Privacy Cross Functional Review. The Privacy Cross Functional Review is covered in further depth in Section 4.
- **Confirming and Communicating Key Privacy Decisions.** The Privacy PM team provides XFN Review feedback to product teams and works with them to finalize privacy design decisions.
- **Tracking Product Launches and Documenting Key Privacy Decisions.** The Privacy PM team maintains the Privacy Launch Calendar, covered in more detail in Section 5.
- **Communicating Privacy Updates to Cross Functional Team.** The Privacy PM Team provides highlights and upcoming launch updates to the XFN Review team and other employees.
- **Maintaining the Internal Privacy Wiki.** The Privacy PM team maintains the internal privacy wiki, which contains information regarding Office Hours, Training, Contact Information, and other privacy resources.

3. Privacy Training.

The Privacy PM team holds monthly training sessions, and sessions as requested for teams. These training sessions are open to everyone at Facebook, but Product Managers and product engineers, in particular, are encouraged to attend. The purpose of these trainings is to educate employees on Facebook’s privacy framework, its obligations to users, and the privacy resources available to them. The training covers:

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

4. The Privacy Cross Functional Review.

The Privacy Cross Functional Review Team (the “Privacy XFN”) reviews privacy-related products (settings and education) as well as privacy features of all Facebook products, and, in certain instances, privacy-related bugs. An issue, product, or feature may be reviewed more than once and at different stages.

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

5. Launch Calendar, Reports and Records

The Privacy PM team uses several methods to track and record the Privacy Review Process:

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

An Overview of the Privacy Review Flow:

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

Privacy Process Overview

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

Exhibit C

Title	Department
Chief Security Officer	Security
Software Engineer	Security
Chief Privacy Officer	Product
Head of Privacy Program	Privacy Product Management
Privacy Program Manager	Privacy Product Management
Privacy Program Manager	Privacy Product Management
Privacy Program Manager	Privacy Product Management
Privacy Program Manager	Privacy Product Management
Lead Privacy Program Manager	Privacy Product Management
VP Technology Communications	Communications
Technology Communications Director	Communications
VP & Deputy General Counsel	Legal
Associate General Counsel, Privacy	Legal
Associate General Counsel, Head of Data Protection	Legal
Program Manager, Privacy/Data Protection	Legal
Associate General Counsel, Privacy & Product	Legal
Privacy & Product Counsel	Legal
Privacy & Product Counsel	Legal
Privacy & Product Counsel	Legal
Associate General Counsel, Advertising and Marketing	Legal
Lead Advertising & Privacy Counsel	Legal
VP Product Marketing	Product-Platform Marketing
Product Marketing Manager	Monetization Product Marketing
Product Marketing Manager	Product-Platform Marketing
VP Corporate Comm & Public Policy	Communications
Chief Privacy Officer	Policy
Privacy & Public Policy Manager	Privacy & Public Policy
Technical Privacy Manager	Privacy & Public Policy
Policy Communications Manager	Privacy & Public Policy
Policy Communications Director	Communications
Quantitative Research Manager	Data Science
Engineering Director	Engineering
Policy Manager	Privacy & Public Policy
Developer Policy Enforcement Manager	Developer Operations
Product Manager	Site Integrity
Content Strategy Manager	Content Strategy
Highlight = Member of the Privacy Governance Team	

Exhibit D

Exhibit E

Exhibit F

Exhibit G

Exhibit H

Exhibit I



Facebook Vendor Security

Web Application Security Review

Application Name	
Facebook Sponsor	
Vendor Name	
Vendor Contact/Role	

Pre-flight checklist for Facebook sponsor:

- ✓ Make sure you have engaged with Vendor Security team at least two weeks prior to go-live of application.
- ✓ Make sure vendor is aware that a security assessment may be performed.
- ✓ Ensure you have completed section 1.
- ✓ Ensure sections 2 and 3 are completed by the vendor
- ✓ Ensure section 4 is completed by the vendor if confidential or regulated data is included.
- ✓ Ensure the vendor will provide a stable environment that is the same as their production instance to test the application.
- ✓ Ensure the vendor will provide test credentials/roles/data to test their application.

What is the purpose of this document?

At Facebook, we enjoy building great relationships with awesome vendors. For us to partner with you to represent our brand or process our data, there are some baseline security requirements that need to be fulfilled. We do this because we care deeply about the security of our customers, our employees and our brand, and we need to make sure that you care too.

This form allows us to quickly capture the information that we need to start our review process, provides you with some key items that we will assess, and aims to surface any red flags as early as possible in the process. Fundamentally, we want you to pass our security review, and we're open to discussion with regards to any ways in which we can help.

Who completes this form?

This form is completed partly by the Facebook sponsor (usually the person driving the project), and partly by the vendor. It's OK to send it back and forth via email. If you want to encrypt anything that you send to us, you'll find our [GPG key](#) at the bottom of this document.

What happens next?

The information will be reviewed by the Facebook sponsor, and Facebook’s information security team. Generally, Facebook will want to perform our own security test of the application, and if the answers indicate that the vendor is ready, we’ll get in touch to arrange the timing and scope.

We’ll be 100% transparent with the outputs of our testing, we’ll have a rational conversation with you about any exceptions that we find, and we’ll do what we can to help you if any retesting will be required.

How long will the assessment take?

Once we receive the completed form (or as complete as possible), Facebook will provide an initial response within 2 days. We will work with the vendor to schedule a time to perform the security assessment. Our expectation is that the Facebook sponsor will brief the vendor on ensuring that their application is stable and ready for testing. A vendor assessment will typically take 1 week, but this time may increase depending on a variety of technical factors. We will advise you of any extension in the testing time needed.

What do you do with the results?

We will analyze the results to rate the severity of the issues found during the testing. We recognize that every system can be compromised; perfect security is an illusion. We will take a risk-driven approach to analyzing each finding. You will be informed of the results from the security assessment and will be given an opportunity to comment on each finding.

Answering the questionnaire

The vendor must answer each question as completely and accurately as possible. If the vendor needs to share supporting documentation they should provide it to the Facebook sponsor to be included with this form. If the vendor has results from previous security assessments they should share them with the Facebook sponsor. We believe in open, transparent and honest communication; please adopt the same approach in completing the questionnaire.

Section 1 – What is this application?

This section is completed by the Facebook sponsor, with the aim of understanding the context of the new system and the types of data that are processed.

Section 1: What is this application?	
(To be completed by the Facebook sponsor)	
1.1	What is this application going to do for us? Does it replace an existing system?

	Guidance: High level is OK – it could be a marketing site for a specific event, it could be system that processes our financials – assume that we know nothing.
1.2	Do we have an existing contractual relationship with this vendor?
	Guidance: If so, what was that for? We can pull the existing contract and make sure that it has the right security provisions.
1.3	Based on our <u>data classification policy</u>, what's the most sensitive class being handled by this application? Give some examples of the types of data.
	Guidance: We obviously care about some things more than others. If the data type is classified or regulated, there are a few extra boxes that we need to check. You can check the data classifications that we use at http://fburl.com/dataclass .
1.4	What integrations are required into other Facebook systems?
	Guidance: For example, a feed from HR, a SAML integration, etc. Note that if >20 employees will use this application, you will be required to integrate with an existing user store (SAML or FBConnect).
1.5	Who from Facebook will have access? How will you provision and manage accounts?
	Guidance: For example, 'everyone in marketing', 'just the helpdesk', 'only me', etc.
1.6	When do you expect to go live?
	Guidance: Generally speaking, we can turn around a security assessment within a week, but if issues are found during the review it can cause delays while the vendor fixes the problem.

Section 2 – Operational Details

This section is completed by the vendor, with the aim of making us feel good about how the service will be managed for the duration of our relationship.

Section 2: Operational Details	
(To be completed by the vendor)	
2.1	What process will be followed to maintain up to date patch levels? Who owns making sure that this happens?

	Guidance: You should have a process by which you are actively seeking new vulnerabilities in your infrastructure, with clear responsibility for fixing them.
2.2	What process will be followed to control access to our data on the back end? Who will have access, and how will you manage their credentials?
	Guidance: Granting of access should be based on least privilege, access credentials should be suitably protected, and revoked when no longer needed.
2.3	Please describe your process for detecting security events (for example unauthorized access). How you will escalate these events to Facebook?
	Guidance: You will need to have a way of detecting security events. We can be prescriptive on notification methods, but in most cases an email or phone call is fine.
2.4	Please provide the primary URL for your application, and public IP addresses for the hosting environment.
	Guidance: We won't start testing anything without talking to you first. Note - if you have a testing environment ready for us now, please provide details and credentials here.
2.5	Please provide details of any existing third party security testing that you have performed.
	Guidance: If you have existing 3 rd party audits (for example an SSAE16 or a web application penetration test), please share details and attach whatever outputs you can share to your response. The more you can share, the less we have to test.

Section 3- Vendor Checklist

This section is completed by the vendor – just validate that the statement is true, then check the box! A positive response is required for each of these questions – they cover the most common types of web vulnerabilities, mostly drawn from the OWASP Top 10, with a few extras that we frequently see being used as attack vectors against our vendors. **We understand the pressure to quickly check each box, but please understand that we will test for each of these items. If it's obvious from our testing that you have not really done your own testing, we will not do business with you.** Our goal is for you to have visibility into what we test for, and to give you a chance to remediate these items in advance of our tests.

Section 3: Vendor Checklist

(To be completed by the vendor)		
3.1	You have tested all application endpoints that interact with a backend data store for injection vulnerabilities.	<input type="checkbox"/>
	Guidance: The most common form of injection that would cause an audit failure would be SQL injection. Detailed testing and remediation guidance can be found at https://www.owasp.org/index.php/Top_10_2010-A1	
3.2	You have tested all application endpoints that accept user input for cross-site scripting vulnerabilities.	<input type="checkbox"/>
	Guidance: The preferred option is to properly escape all untrusted data. Detailed testing and remediation guidance can be found at https://www.owasp.org/index.php/Top_10_2010-A2	
3.3	You have tested all application endpoints for unvalidated redirects.	<input type="checkbox"/>
	Guidance: Where possible, don't allow redirects. If that's not possible, detailed testing and remediation guidance can be found at https://www.owasp.org/index.php/Top_10_2010-A10	
3.4	All application endpoints that pass authentication credentials or session tokens are only accessible via HTTPS, using SSLv3 or above.	<input type="checkbox"/>
	Guidance: Any page that requires authentication credentials or passes session tokens should only be available over HTTPS. Guidance on testing your SSL version can be found at https://www.owasp.org/index.php/Testing_for_SSL-TLS_(OWASP-CM-001)	
3.5	All session cookies are marked as secure and HTTPOnly.	<input type="checkbox"/>
	Guidance: Detailed testing and remediation guidance can be found at https://www.owasp.org/index.php/HttpOnly and https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OWASP-SM-002)	
3.6	Any application endpoint that executes an action on behalf of an authenticated user is protected from cross-site request forgery via the inclusion of an unpredictable token in a hidden field.	<input type="checkbox"/>
	Guidance: Detailed testing and remediation guidance can be found at https://www.owasp.org/index.php/Top_10_2010-A5	
3.7	Any application endpoint that requires the user to enter their credentials is protected from clickjacking via the use of the 'X-FRAME-OPTIONS' header.	<input type="checkbox"/>
	Guidance: Detailed testing and remediation guidance can be found at https://www.owasp.org/index.php/Clickjacking	
3.8	Any passwords stored by your application are hashed with a standard hashing algorithm and an appropriate salt.	<input type="checkbox"/>
	Guidance: Detailed testing and remediation guidance can be found at https://www.owasp.org/index.php/Top_10_2010-A7	

3.9	User logins enforce password complexity and are protected from brute forcing by lockout, CAPTCHA, 2nd factor requirements or authentication delays.	<input type="checkbox"/>
Guidance: Detailed testing and remediation guidance can be found at https://www.owasp.org/index.php/Blocking_Brute_Force_Attacks and https://www.owasp.org/index.php/Password_length_%26_complexity		
3.10	You have scanned your network perimeter, disabled any unnecessary services, and patched any critical CVEs in your infrastructure.	<input type="checkbox"/>
Guidance: As an example, you may have scanned your perimeter with nmap (http://nmap.org) , identified all exposed services and their versions, and cross referenced this with the list of critical CVEs at http://cve.mitre.org/index.html		
3.11	You consent to Facebook or their appointed third party testing firm testing your application and infrastructure at any point during our contractual relationship with a minimum of 48 hours of notice.	<input type="checkbox"/>
Guidance: Our vendor security program is a process, not an event. As such, we will continue to perform non-destructive, non-disruptive security testing during the course of our relationship, with adequate notice and prior agreement. However, generally speaking we'll only retest once a year.		
3.12	During your contractual relationship with Facebook, you will agree to respond to any critical security vulnerabilities reported by Facebook within 24 hours.	<input type="checkbox"/>
Guidance: We may occasionally become aware of vulnerabilities in your application, from our own testing, industry news or our bug bounty program. While it's not always possible for bugs to be fixed immediately, we need a commitment that they will be triaged and acted upon within 24 hours.		
If you were unable to check any of the boxes, please provide details here.		
Guidance: You may, for example, have compensating controls. Alternatively you may feel that one or more of these items does not apply to you – please provide as much detail as you can.		

Section 4 – Confidential/Regulated Data Supplement

This section is completed by the vendor – just validate that the statement is true and check the box. Your Facebook contact will tell you if you need to complete this section – in most cases it's not required.

If you are handling Facebook data that we classify as 'confidential' or 'regulated', there are a few more items that we will need from you. A positive response is required for each of these questions.

Section 4: Confidential/Regulated Data Checklist (To be completed by the vendor)		
4.1	You have completed all required regulatory audits (PCI for payment data, SSAE16 for financial data etc.) applicable to the data being processed.	<input type="checkbox"/>
	Guidance: Please attach your audit report(s) when you email this document back to us, under the terms of our existing NDA.	
4.2	You use a reputable third party to assess your application and infrastructure security at least annually. You will share the outputs of this testing with Facebook along with any remediation plans.	<input type="checkbox"/>
	Guidance: The testing should cover OWASP Top Ten type vulnerabilities, and should be performed by a competent security tester as opposed to just an automated scanner. When sharing results with us, it's OK to sanitize anything really sensitive. Please attach outputs from your most recent testing , under the terms on our existing NDA.	
4.3	Your service is hosted in the US or as may be applicable, in the EU. All backup copies of Facebook data remain in the US or EU. Additionally, all staff with access to Facebook data are physically located in the US or EU.	<input type="checkbox"/>
	Guidance: For confidential or regulated data, the data needs to be physically located in the US or EU, and managed entirely by staff in the US or EU.	
If you were unable to check any of the boxes, please provide details here.		
<p>Guidance: You may, for example, have compensating controls. Alternatively you may feel that one or more of these items does not apply to you – please provide as much detail as you can.</p>		

Our GPG Public Key (if you want to encrypt anything that you send to us).

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG/MacPGP2 v2.0.18 (Darwin)

mQENPFCKsF8BCADk84YTSjVC+ik38cbn362A0V8qW9gqsdvdx3kgtzhyoIt12C6
5AFMokvncwXt7H7blyBYNhjFA1ufo1RrZzCAekU1C5+eFXKrbi/tyV4LHvAc3
ARW3kKpAdDlJ0eToQyF8qATWd0Kf10z7Pjprz8VnrCPLHgvdl5umg0jpdT0z
WwqLa0H8rjo+COIT1118PaTe+1+vxgN37p8k151bHbY00eYp85m5J3Cm
xdv67F5EXh2LVOPrnJ9yzLl/hrPuktGtmJpp05D7vmJKYVY04TIv2Q+V+pd/nS
vaH+8SGHM1914//OgRF0hIt788Ac7qTzVPSABEBAAG0J1ZlbnRvcjE8T2M1cm10
eSAsdmVuZG9yc2VjdXJpdHlA2mIuI29tP0kBPwQTAQIARQUKURJ/wtBlwUJdWw/
AAcLCogIawIBBH0I2agKtCWMA9Bh8h4B8h8AAo:EH71eWNTVzVfgr16/0NHGDM
SAX+24Le/9RhbJH9R8eblvc+0T2Tc:8yIjJaMubHjWFRK3ulm7dS7M+GGPkSyo
PUhnFzZrbr9LVnm10FqjVJBHxb2VbA2YL+INfW7Xt+e6Ygk/VBQMk5gduD08vx2
j1o0M1al1KUF1Aph6G8y801P8arWfgy7dVP103+EEHJet9+y4SKhXzPFVBEed
Rke1zVdKXkymz10a76JH0KraoG/5Huf0aE8IAUC8C8y1jJH8+G8Se1zJ58
aBUPFX0dJX3yaNGLT05E14UkA250iRNeVHFkuLCUMB84CG/ue:rMxHEH79/arC1
ToTo/RBQAR0LFJ65AQ0EUKRJ/wEIAMwtL50HmW7nL0D/RqwkD0xdm1eXWGr
dRo+EpJVO/aA02:3Xe7bJW06f01JmCh8Swbb05smjkhDq838Ezmp+an1w0q3
yBlc1cY8eIvNDa3k8GvJgXg22351LDPX7UJ05w+3X0v1S4H0h0K6Dg5KEOV
N3utxo9v4g5B4xV752sqFRK78u78x1ac2s1aBm1BsmIe4F0jvthA9JH99:7oR2
nv6tJLeq4hJDD+Cb8V1hNAXYXC05RPHAMuoyYH0hLr5HMJTe/72kAgbWpyq
7mIXa8F7aw060o3PmC2tu0jJhp1Ae8x0Pm8m5e8mz/7gFOABQ8AAKRAQY
AQIADW0KURJ/wtBlwUJdWw/AAEpCRDE9X1Telc738BdIAQEAQIABg0CURIJ/wAK
CRAAJ7vni1fvwJdRB/49mDTCmJEVb+DwITQBh1DG5f12j1LXQvnhUDHmY2n0v1ko
H8Gh88jkm8771aFf0UngMcqf1F8058yW2G0eua0PC29ELK0g5u7w4Daxh20s
o92MH27zphSKVgTA98bo+2LRtGF1K25vRv1B8W16kHtveIKR00w1D8EppC5t4
```

Exhibit J

Exhibit K

Data Use Policy

Date of Last Revision: December 11, 2012

Information we receive and how it is used

- [Information we receive about you](#)
- [Public information](#)
- [Usernames and User IDs](#)
- [How we use the information we receive](#)
- [Deleting and deactivating your account](#)

Sharing and finding you on Facebook

- [Control each time you post](#)
- [Control over your timeline](#)
- [Finding you on Facebook](#)
- [Access on phones and other devices](#)
- [Activity log](#)
- [What your friends and others share about you](#)
- [Groups](#)
- [Pages](#)

Other websites and applications

- [About Facebook Platform](#)
- [Controlling what information you share with applications](#)
- [Controlling what is shared when the people you share with use applications](#)
- [Logging in to another site using Facebook](#)
- [About social plugins](#)
- [About instant personalization](#)
- [Public search engines](#)

How advertising and Sponsored Stories work

- [Personalized ads](#)
- [Ads + social context](#)
- [Sponsored stories](#)
- [Facebook content](#)

[Cookies, pixels and other similar technologies](#)

[Some other things you need to know](#)

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 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 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 the computer, mobile phone or other device you use to access Facebook, including when multiple users log in from the same device. This may include your IP address and other information about things like your internet service, location, the type (including identifiers) of 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.

- 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.

We also put together data from the information we already have about you and your friends. For example, we may put together data about you to determine which friends we should show you in your News Feed or suggest you 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 that you might be interested in. We may also put together data about you to serve you ads 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 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 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 it. 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

A Username (or Facebook URL) is a custom link 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. 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 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 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 the other photos 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" 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 an 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.

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 or change the audience of content you post.

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 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.

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.

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, it won't be able to continue to update the additional information you've given them permission to access. 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 to delete the information you've already shared with them, you should contact the application and ask them to delete it. Visit the application's page on Facebook or their 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” 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.

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 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 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.

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 “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 advertising and Sponsored Stories work

Personalized ads

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 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 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; 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](#)", 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
[About](#)[Create Ad](#)[Create Page](#)[Developers](#)[Careers](#)[Privacy](#)[Cookies](#)[Terms](#)[Help](#)

Exhibit L

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.

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 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 ads and commercial content that are 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 in connection with that content, subject to the limits you place.
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 our software, such as a stand-alone software product or a browser plugin, you agree that from time to time, the software may download 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 a state or federal court located in Santa Clara County. 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.
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, 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.

[About](#)[Create Ad](#)[Create Page](#)[Developers](#)[Careers](#)[Privacy](#)[Cookies](#)[Terms](#)[Help](#)

Exhibit M

Facebook Platform Policies

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.

[Additional Languages](#)

Introduction

Date of Last Revision: April 9, 2013

Facebook Platform is an extension of Facebook, whose mission is to make the world more open and connected.

Platform applications and developers are required to comply with, and are subject to, the following documents:

- [Statement of Rights and Responsibilities](#): requirements for anyone who uses Facebook.
- [Principles](#): the spirit of the law for Platform.
- [Policies](#): the letter of the law for Platform.

Here are some [Examples and Explanations](#) for specifics.

Principles

Create a great user experience

- Build social and engaging applications
- Give users choice and control
- Help users share expressive and relevant content

Be trustworthy

- Respect privacy
 - Don't mislead, confuse, defraud, or surprise users
 - Don't spam - encourage authentic communications
-

Policies

I. Features and Functionality

1. You must not violate any law or the rights of any individual or entity, and must not expose Facebook or Facebook users to harm or legal liability as determined by us in our sole discretion. In particular you will (if applicable): 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.
2. You must not include functionality that proxies, requests or collects Facebook usernames or passwords.
3. You must not circumvent (or claim to circumvent) our intended limitations on core Facebook features and functionality.
4. If you offer a service for a user that integrates user data into a physical product (such as a scrapbook or calendar), you must only create a physical product for that user's personal and non-commercial use.
5. If you exceed, or plan to exceed, any of the following thresholds please [contact us](#) as you may be subject to additional terms: (>5M MAU) or (>100M API calls per day) or (>50M impressions per day).
6. Your website must offer an explicit "Log Out" option that also logs the user out of Facebook.
7. Special provision for apps on Pages: When a user visits your Page, if they have not given explicit permission by authorizing your Facebook app or directly providing information to your Page, you may only use information obtained from us and the user's interaction with your Page in connection with that Page. For example, although you may use aggregate analytics for your individual Page, you must not combine information from any other sources to customize the user's experience on your Page and may not use any information about the user's interaction with your Page in any other context (such as analytics or customization across other Pages or websites).
8. You must not use or make derivative use of Facebook icons, or use terms for Facebook features and functionality, if such use could confuse users into thinking that the reference is to Facebook features or functionality.
9. Mobile Web Apps that are running within the Facebook iOS app must not accept payments. In particular, these apps must not reference, use, or otherwise encourage the use of Facebook Payments or other non-iOS approved payment methods.
10. Reciprocity and Replicating core functionality: (a) Reciprocity: Facebook Platform enables developers to build personalized, social experiences via the Graph API and related APIs. If you use any Facebook APIs to build personalized or social experiences, you must also enable people to easily share their experiences back with people on Facebook. (b) Replicating core functionality: You may not use Facebook Platform to promote, or to export user data to, a product or service that replicates a core Facebook product or service without our permission.
11. The primary purpose of your Canvas or Page Tab app on Facebook must not be to simply redirect users out of the Facebook experience and onto an external site.
12. You must not include data obtained from us in any search engine or directory without our written permission.
13. Special provisions for games:
 - a. Desktop web games off of [Facebook.com](#) may only use Facebook Login ([Authentication](#), excluding user connections such as friend list), [Social Plugins](#) and publishing (e.g., Feed Dialog, Stream Publish, or Open Graph). When authenticating, these games may not request [additional permissions](#) other than age, email, and our [Publishing Permissions](#).
 - b. Games on [Facebook.com](#) and mobile must not share the same app ID with desktop web games off of [Facebook.com](#). You must not use [Canvas](#) apps to promote or link to game sites off of Facebook, and must not use emails obtained from us to promote or link to desktop web games off of [Facebook.com](#).
 - c. Games on [Facebook.com](#) or Mobile Web must use Facebook Payments as their sole and exclusive payment method for all virtual goods and currencies made available to users within the game. All other payment options are prohibited within games on [Facebook.com](#) or Mobile Web unless they go through Facebook Payments rather than directly through that payment option. By "Payment Method" we mean any method that allows a user to complete a transaction in a game that is on [Facebook.com](#) or Mobile Web, including, without limitation, by exchanging monetary value for virtual currency or virtual goods, whether directly at the time of purchase or via any

previous transaction such as the user's earlier purchase of a prepaid gift card or electronic code. In-game rewards of virtual currency or virtual goods earned by users through game-play activity alone are exempt from this definition.

d. Games on [Facebook.com](https://www.facebook.com) or Mobile Web may reward users with virtual currency or virtual goods in exchange for user actions that do not involve third parties, but rewards for user actions that involve third parties must be powered by Facebook Payments by integrating Facebook Payments offers. For example, you may not reward users with virtual currency or virtual goods in exchange for any action in which personally identifiable information is shared with a third party, you may not reward users with virtual currency or virtual goods in exchange for third party downloads, such as toolbars or ringtones, and you may not reward users with virtual currency for engaging in passive actions offered by third parties, such as watching a video, playing a mini-game, or taking an anonymous poll.

II. Storing and Using Data You Receive From Us

1. You will only request the data you need to operate your application.
2. You may cache data you receive through use of the Facebook API in order to improve your application's user experience, but you should try to keep the data up to date. This permission does not give you any rights to such data.
3. 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. In addition, you will include your privacy policy URL in the App Dashboard, and must also include a link to your app's privacy policy in any app marketplace that provides you with the functionality to do so.
4. Until you display a conspicuous link to your privacy policy in your app, any data accessed by your app (including basic account information) may only be used in the context of the user's experience in that app. A user's friends' data can only be used in the context of the user's experience on your application.
5. Subject to certain restrictions, including on use and transfer, users give you their basic account information when they connect with your application. For all other data obtained through use of the Facebook API, you must obtain explicit consent from the user who provided the data to us before using it for any purpose other than displaying it back to the user on your application.
6. You will not directly or indirectly transfer any data you receive from us, including user data or Facebook User IDs, to (or use such data in connection with) any ad network, ad exchange, data broker, or other advertising or monetization related toolset, even if a user consents to such transfer or use. By indirectly we mean you cannot, for example, transfer data to a third party who then transfers the data to an ad network. By any data we mean all data obtained through use of the Facebook Platform (API, Social Plugins, etc.), including aggregate, anonymous or derivative data.
7. You will not use Facebook User IDs for any purpose outside your application (e.g., your infrastructure, code, or services necessary to build and run your application). Facebook User IDs may be used with external services that you use to build and run your application, such as a web infrastructure service or a distributed computing platform, but only if those services are necessary to running your application and the service has a contractual obligation with you to keep Facebook User IDs confidential.
8. If you need an anonymous unique identifier to share outside your application with third parties such as content partners, advertisers, or ad networks, you must use our mechanism. You must never share this anonymous unique identifier with a data broker, information broker, or any other service that we may define as such under our sole discretion.
9. You will not sell or purchase any data obtained from us by anyone. 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 data outside your application.
10. If you stop using Platform or we disable your application, you must delete all information about a user you have received from us unless: (a) it is basic account information; or (b) you have received explicit consent from the user to retain their data.
11. You cannot use a user's friend list outside of your application, even if a user consents to such use, but you can use connections between users who have both connected to your application.

12. You will delete all data you receive from us concerning a user if the user asks you to do so, and will provide an easily accessible mechanism for users to make such a request. We may require you to delete data you receive from the Facebook API if you violate our terms.
13. You will not include data you receive from us concerning a user in any advertising creative, even if a user consents to such use.
14. You must not give your secret key and access tokens to another party, unless that party is an agent acting on your behalf as an operator of your application. You are responsible for all activities that occur under your account identifiers.

III. Content

A. General

1. Responsibility for content: You are responsible for all content of and within your application, including advertisements, user-generated content, and any content hosted, streamed or otherwise delivered to users by third parties. You must make it clear that this content is not provided by Facebook. You must also comply with the [Facebook Community Standards](#).
2. Demographic restrictions: You are responsible for restricting access to your content in accordance with our content policies and all applicable laws and regulations. Although we [provide controls](#) to assist with this, please note that we make no representations regarding the sufficiency of any controls provided to you and that you are ultimately responsible for establishing legally compliant restrictions for each country where your app is visible.
3. Advertisements and cross-promotions:
 - a. You must not include advertisements, cross-promote other applications, or provide web search functionality in content distributed through [Facebook social channels](#).
 - b. You can only utilize advertising or similar monetization related products or services from companies that appear on this [list of Advertising Providers](#) within [Apps on Facebook.com](#).
4. Promotions: If you run, reference, or facilitate a promotion (contest, competition, or sweepstake) on Facebook, you must comply with Facebook's [Promotions Guidelines](#).
5. Permission from Facebook: You must not promote, or provide content referencing, facilitating, or containing online gambling, online real money games of skill or online lotteries without our written permission.
6. Quality of content: you are responsible for providing users with a quality experience and must not confuse, defraud, mislead, spam or surprise users. For example, you must monitor your app's negative feedback in [Application Insights](#) to ensure it stays below our thresholds, avoid excessive advertisements or bugs, and ensure the description of your app is consistent with your app's content.

B. Content Rights

1. You agree that you will not promote or provide content that references, facilitates, contains or uses content that infringes upon the rights of any third party, including intellectual property rights, privacy, publicity, moral or other personal or proprietary rights, or that is deceptive or fraudulent.
2. You must ensure that you own or have secured all rights necessary to copy, display, distribute, deliver, render and publicly perform all content of or within your application to Facebook users in all countries where you make the content available.
3. You are responsible for all licensing, reporting and payout obligations to third parties required in connection with content of or within your application.
4. You must use commercially reasonable geo-filtering technology to block access to your application's content in countries where you are unauthorized to deliver such content, or where delivery of such content would otherwise infringe the rights of a third party.
5. Although we have no obligation to do so, in our sole discretion we may request, and you are required to provide us, proof that your application and any content of or within your application is properly licensed.

C. Third Party Content

If your application contains content submitted or provided by third parties, you must comply with the following rules:

1. In the United States you must take all steps required to fall within the applicable safe harbors of the Digital Millennium Copyright Act including designating an agent to receive notices of claimed infringement, instituting a repeat infringer termination policy and implementing a "notice and takedown" process. In other countries, you must comply with local copyright laws and implement an appropriate "notice and takedown" process upon receiving a notice of claimed infringement.

IV. Application Integration Points

1. You must not incentivize users to use (or gate content behind the use of) Facebook social channels, or imply that an incentive is directly tied to the use of our channels.
2. You must not pre-fill any of the fields associated with the following products, unless the user manually generated the content earlier in the workflow: Stream stories (user_message parameter for Facebook.streamPublish and FB.Connect.streamPublish, and message parameter for stream.publish), Photos (caption), Videos (description), Notes (title and content), Links (comment), and Jabber/XMPP.
3. If a user grants you a publishing permission, actions you take on the user's behalf must be expected by the user and consistent with the user's actions within your app.
4. Platform integrations, including social plugins:
 - a. Your advertisements must not include or be paired with any Platform integrations, including social plugins such as the Like button, without our written permission.
 - b. You must not sell or purchase placement of our Social Plugins, and must not facilitate or participate in any like exchange program.
 - c. You must not incentivize users to Like any Page other than your own site or application, and any incentive you provide must be available to new and existing users who Like your Page.
 - d. You must not obscure or cover elements of our social plugins, such as the Like button or Like box plugin.
 - e. Ad networks, ad exchanges, and data brokers must not use Facebook's Platform, logos, and trademarks (including, but not limited to, Platform APIs, social plugins, the Share button, and the F logo).
5. Facebook messaging (i.e., email sent to an @facebook.com address) is designed for communication between users, and not a channel for applications to communicate directly with users.
6. Requests: you may not offer a select all option or pre-select multiple recipients to receive a Request (effective October 2, 2013).

V. Enforcement

We can take enforcement action against you and any or all of your applications if we determine in our sole judgment that you or your application violates Facebook Platform Terms and Policies. Enforcement action is both automated and manual, and can include disabling your application, restricting you and your application's access to Platform functionality, terminating our agreements with you, or any other action as we in our sole discretion deem appropriate.

Communication with developers takes place via an email sent from the facebook.com or facebookmail.com domain to the contact email address registered to the application. To stay in touch, please ensure that your email address is current and that you do not filter out any such messages.

VI. Changes

We can change these Platform Policies at any time without prior notice as we deem necessary. Your continued use of Platform constitutes acceptance of those changes.

VII. Definitions

1. By "Application" we mean canvas page application, Platform integration, or any other technical integration we have assigned an application identification number.
2. By "Facebook social channel" we mean Application Info Section, Page Tab, Feed, Requests (including invites), inbox attachments, Chat, Cover, Bookmarks, or any other feature of a user profile or Facebook communication channel in which or through which an application can provide, display, or deliver content directed at, on behalf of, or by permission of a user.
3. By "basic account information" we mean: name, email, gender, birthday, current city, and profile picture URL.
4. By "Facebook Platform Terms and Policies" we mean the Statement of Rights and Responsibilities and the Platform Policies.
5. By "User data you receive from Facebook" we mean any data or content (including any images, text, or other information or materials) you receive from us, that was provided by users to us, or was associated by us with a particular user.

VIII. Branding and Promotion Policy

1. You must follow the guidelines set forth in the [Facebook Brand Resource and Permissions Center](#).
2. Your app's description, display name and icons must adhere to our [Advertising Guidelines](#).

IX. Advertising Guidelines

X. Facebook Developer Payments Terms

Developers participating in the program for accepting payments are subject to [these terms](#).

XI. Ads API

1. Separate apps: You must use separate apps for your staging, self-service, managed service, and white-labeled apps. If you offer a white-label version of your app, you must only do so by creating a unique app for each end-advertiser (or requiring each end-advertiser to create their own app) and you must include a required field for the third party to agree to Facebook's Platform Policies.
2. Separate ad accounts: You must use separate ad accounts for each end-advertiser and use our multi-client manager functionality to structure your end-advertiser accounts. You must never combine multiple end-advertisers within the same ad account, and this includes their Facebook connections (ex: pages and apps).
3. Freemium: If you offer a free or trial version of an ads API app, you must allow no more than 50 ad creations per day per customer, require phone or email verification for all new accounts, and prohibit affiliate networks from using your technology.
4. Pricing transparency: You must only charge fees for the use of your tools and managed services, and must only do so on a fixed fee (per campaign or period) or variable percentage of ad spend. You must disclose to your clients the actual amount that you spent on Facebook advertising based on the auction pricing, including the actual Facebook metrics (e.g. CPC, CPM rate) and the amount you charged as fees. We reserve the right to disclose this information to your client upon their request. We may require documentation from you to ensure your compliance with this policy.
5. Data collection and use:
 - a. You may place 1x1 pixel view tags on certain advertisements with our prior authorization.

- b. All data collected or obtained by you or the end-advertiser, including but not limited to all view tag data that is not otherwise available through the Facebook service, and all data derived therefrom, may only be used by you or the end-advertiser on an anonymous basis to optimize and measure the performance of that end-advertiser's Facebook campaign. Neither you nor the end-advertiser may use data for the following purposes: retargeting whether on or off of the Facebook service; to commingle data across an advertiser's campaigns from multiple platforms; to build or augment any user profiles, or to use piggybacking or redirects with the 1x1 pixel tags, or for any other purpose not expressly authorized by us.
- c. You must not permit any person (other than an agent acting on the end-advertiser's behalf) to access the end-advertiser's Ad or Sponsored Story advertising statistics, including but not limited to, fixed CPM rates and any other raw, aggregate, or anonymous statistics derived from this data.
- 6. **Separate Reporting:** If you use last-click attribution, create reporting tools that separate Facebook reporting from other channels. For example, don't create reporting dashboards that directly compare Facebook Ads metrics to search or display marketing metrics on a last-click basis. If you support other channels, you must either create a separate Facebook tool, include Facebook metrics in a separate Facebook section of your tool, or show multi-touch attribution results side-by-side with last-click attribution results. You may report Facebook mobile ads ROI metrics as they relate to other mobile ads channels.
- 7. **Self-service reporting for Homepage ads:** You must include a self-service reporting dashboard, through which end-advertisers may access up-to-date reports (raw ad statistics) for all available data points of their Homepage Ad and Sponsored Story campaigns.
- 8. **Bidding types:** You must implement all bidding types, including Optimized CPM, and you must not default to a specific type (ex: you must not default to CPC and hide oCPM).
- 9. **Custom Audiences:**
 - a. If you use custom audiences you must comply with the [Custom Audience Terms](#).
 - b. You may create a custom audience on a client's behalf but must only use the client's customer data to do so (ex: you must not collect or provide any additional data to create a custom audience).
 - c. You must not use Facebook User IDs to create custom audiences unless the person associated with the User ID has logged into your client's app and your client has secured any necessary consent from that person (ex: you must not create a custom audience based on users who have engaged with a Facebook Page).
 - d. You must not sell custom audiences, and must not transfer a custom audience to anyone without our permission.
 - e. Your custom audience tool may provide the same functionality and targeting options that Facebook provides, but you must not provide additional data or targeting options.
- 10. **Enforcement:** You must immediately revoke an end-advertiser's access to your app upon our request.

Examples and Explanations

We want you to be successful on Facebook Platform, and we believe that the best way to do so is to provide a great user experience. Our Platform Policies will help you do this by explaining what's required; these [examples and explanations](#) will help you understand how to put that into practice.

Additional Languages

العربية 中文(香港) 中文(台灣) Deutsch Español Français עברית
 Italiano 日本語 한국어 Polski Português (Brasil) Türkçe

July 14, 2015

VIA EMAIL AND FEDERAL EXPRESS

Laura D. Koss, Esq.
Reenah L. Kim, Esq.
Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, DC 20850

Re: *In re Facebook, Inc.*, FTC Docket No. C-4365

Dear Mses. Koss and Kim:

We received your letter dated June 4, 2015 seeking clarification of the scope of Facebook's assessment ("the Assessment") for the period from February 12, 2013 to February 11, 2015 (the "Assessment Period") pursuant to the Agreement Containing Consent Order ("the Order"), particularly with respect to entities acquired by Facebook during the Assessment Period. This letter endeavors to provide information regarding the processes assessed as they relate to acquisitions. PricewaterhouseCoopers LLP ("PwC") has also provided a letter explaining its approach to acquisitions in its Assessment.

Please note that material contained in this response constitutes Facebook's confidential business information and should be treated with the highest degree of confidentiality pursuant to 5 U.S.C. §§ 552(b)(3) & (b)(4) and 15 U.S.C. § 46(f).

Facebook's Privacy Program is designed to address privacy risks related to the development, management, and use of new and existing Facebook products and the information of Facebook's users. The Order limits the scope of the required assessment to evaluating the practices of Facebook, Inc. However, as will be explained further below, Facebook assesses and addresses the impact of every acquisition on Facebook's Privacy Program and incorporates acquired entities into its formal Privacy Program controls where appropriate.

Facebook's Privacy Program is defined by nine assertions which are supported by 61 controls designed to ensure that Facebook achieves its privacy objectives. To the extent that an acquired entity's technology, product, or feature is integrated into products or services for Facebook consumers, those acquired entities are subjected to Facebook's formal Privacy Program. Documentation of the Privacy Program controls was made available to PwC in

performing its examination, including documentation of the controls as applied to integrated acquired entities. Moreover, even those acquired entities that continued to operate independently of Facebook after acquisition engaged with Facebook's Privacy Program and benefited from a number of controls tested by PwC.

Overview of Facebook's Acquisitions

Facebook's acquisitions come in different shapes and sizes; they include purely talent acquisitions, as well as tech-related acquisitions, and acquisitions of companies that will operate as independent affiliates. Each acquired entity is unique with respect to the nature of its business or technology and the ways in which it is integrated into Facebook products and features. Each acquired entity is therefore also unique with respect to any potential privacy implications it poses and the nature and degree of privacy-related review needed. As will be discussed further below, this means that there are some controls that are applicable to all acquired entities, while there are other controls that are only relevant to certain kinds of acquired entities due to the nature of their engagement with Facebook products and features.

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

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

After

acquisition, acquired entities continue to be subject to applicable controls to the extent they impact Facebook's Privacy Program. For example:

Onboarding and Provisioning. Acquired entities are typically subject to several controls related to onboarding employees and provisioning equipment, including background checks and training.

Security Controls and Security Risk Assessments. Ongoing security-related controls are applied to any acquired entity that utilizes or poses a threat to Facebook infrastructure or data.

Ongoing XFN Review. (b)(4); (b)(3):6(f)

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

Privacy Risk Assessments and the Privacy Summit. Facebook considers privacy risks as part of its Privacy Risk Assessments and its Privacy Summits, including those risks introduced by acquired entities.

A key feature of Facebook's Privacy Program is that, in addition to top-down privacy assessments like the Privacy Summit, the program provides for identifying and escalating

privacy issues from the ground-up. Various team members that are either part of or strategically assigned to a number of Facebook engineering, product development, and security teams (to name a few), are specifically tasked with recognizing privacy issues and driving them into the Privacy Program processes. As a result, the application of the Privacy Program controls to Facebook's acquired entities derives directly from the nature of an acquired entity's products and operations and the extent to which its integration with Facebook products, features, data, or infrastructure implicates privacy processes. Some Privacy Program controls may apply to acquired entities. Others are only applicable to certain kinds of acquired entities because of these differences in their degree of integration. (b)(4); (b)(3):6(f)

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

Onboarding and Provisioning

Facebook's onboarding processes are designed to ensure that employees, including those gained through an acquisition, have the proper background and incentives to protect Facebook's systems and consumer information.

Prior to accessing Facebook's systems or data, personnel employed by acquired entities and affiliates are subject to many of the same policies as Facebook employees. (b)(4); (b)(3):6(f)

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

Facebook provides laptops to employees of its acquired entities. (b)(4); (b)(3):6(f)

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

Security Controls and Risk Assessments

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

Specifically, to the extent an acquired entity uses Facebook's infrastructure for its own technology or its employees have access to Facebook infrastructure, it is subject to the following security mechanisms: (b)(4); (b)(3):6(f)

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

All of these mechanisms apply to risks posed to Facebook's infrastructure or data by acquired entities and affiliates. (b)(4); (b)(3):6(f)

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

Ongoing XFN Review

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

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

Privacy Risk Assessments and Privacy Summits

In its annual Privacy Risk Assessments, Facebook identifies reasonably foreseeable, material risks, both internal and external, that could result in Facebook's unauthorized collection, use, or disclosure of covered information, and assesses the sufficiency of any safeguards in place to control these risks. As a part of this process, Facebook considers all risks to Facebook, including those introduced by its acquired and affiliate entities, as well as the processes needed to address those risks.

Facebook also dedicates considerable attention to acquisitions, and to its acquired and affiliate

entities, in its annual privacy summits (“Privacy Summits”), during which key representatives from the Privacy XFN team review and update the Risk Assessment, consider the sufficiency of existing controls, and recommend changes to the Privacy Program. The Summits sometimes involve specific consideration of the acquisitions from the past year or the acquisitions that may take place in the year to come. Sometimes, the Summit involves an entire panel or full session on key acquisitions and lessons learned or areas for monitoring or improvement, both substantively and from a process perspective. In particular, the Summits have addressed key issues relevant to acquired and affiliate entities such as data sharing and integration and training of new employees.

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

* * *

Sincerely,

Edward Palmieri
Director and Associate General Counsel, Privacy



VIA EMAIL

Mr. Edward Palmieri
Director and Associate General Counsel, Privacy
Facebook, Inc.
1299 Pennsylvania Avenue, NW Suite 800
Washington, DC 20004

July 14, 2015

Dear Edward:

As a follow-up to our recent conversation, we are providing you with additional information as requested by the Federal Trade Commission (“FTC”) in their letter to you dated June 4, 2015. Specifically, the FTC requested that “...PwC verify in detail the extent to which its 2015 Assessment covered, for each entity Facebook acquired during the reporting period, whether and how Facebook addressed the acquisition’s impact on its Privacy Program.” As we have discussed with you, since the letter was addressed to Facebook, Inc. (“Facebook”), our client, we direct our response to the FTC’s request included in that letter to you. We understand that this letter will be forwarded to the FTC Staff along with Facebook’s separate response. PwC has also read your response letter to the FTC, dated July 14, 2015, and it is consistent with our understanding of Facebook’s process to assess the impact of acquisitions on Facebook’s Privacy Program (the “Privacy Program”).

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

As part of its acquisition process, Facebook assesses whether the operations and technology of an acquired entity will be integrated with Facebook or if it will remain independently operated. Facebook made numerous acquisitions during the reporting period. Facebook generally categorizes acquisitions as talent (i.e., employees), technology, or companies that continue to operate independently, though to varying degrees after acquisition. For example, the talent-only acquisitions that occurred during the reporting period were part of Facebook’s Privacy Program as new employees were subject to the onboarding controls of the Privacy Program. (b)(4); (b)(3):6(f)

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

.....
PricewaterhouseCoopers LLP, 600 Grant St., Pittsburgh PA 15219
T: (412) 355 6000, www.pwc.com



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

As the scope of the Order requires a comprehensive privacy program for Facebook, any independently operated affiliates were not included in PwC's assessment of the Privacy Program. Although acquired entities that continued to operate independently of Facebook after acquisition were outside the scope of the assessment, as they integrate and interact with Facebook's products and processes they also engage with controls of Facebook's Privacy Program and are subject to our testing.

When the nature of the acquisition involved talent, talent were on-boarded by Facebook and were subject to the existing Privacy Program controls, (b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f) When the nature of an acquisition included technology that was integrated into a Facebook product or service, or if the Facebook product or service was impacted by the acquired technology, these impacted products or services were subject to existing Privacy Program controls (b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f) Additionally, integrated acquisitions were also subject to the Privacy Program enterprise-wide security controls, (b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f) If acquired companies had relationships with third parties that handle or store user data, these third parties were also subject to the Privacy Program controls (b)(4); (b)(3):6(f)

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

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

Please let me know if there are additional questions. If it would be of assistance to the FTC Staff, we would also be happy to speak with them directly concerning the scope of PwC's work in this regard.

Sincerely,

Joseph V. DiVito, Jr.

Principal

(b)(6)

July 28, 2017

VIA ELECTRONIC AND U.S. MAIL

Reenah L. Kim
Bureau Of Consumer Protection
Division Of Enforcement
Federal Trade Commission
600 Pennsylvania Avenue NW, CC-9528
Washington, DC 20580

RE: *In the Matter of Facebook, Inc., Docket No. C-4365*

Dear Ms. Kim:

Thank you for your letter dated June 1, 2017 acknowledging receipt of the Biennial Independent Assessor's Report on Facebook's Privacy Program ("2017 Assessment"), which was submitted for the period February 12, 2015 to February 11, 2017 pursuant to the Agreement Containing Consent Order File No. 0923184. Your letter requested clarification regarding the scope of the 2017 Assessment with respect to Facebook's acquired entities and affiliates. Specifically, we understand you to be asking for confirmation that, as part of the 2017 Assessment, PricewaterhouseCoopers LLP ("PwC") evaluated whether and how Facebook's acquisitions during the reporting period impacted its Privacy Program by testing the application of Facebook's Privacy Program controls to acquired entities. This letter describes and confirms that Facebook, Inc. ("Facebook") assessed the impact of its acquisitions on its Privacy Program and that PwC tested (1) Facebook's process for assessing the impact of its acquisitions, as well as (2) the application of Facebook's privacy controls to acquisitions. Material contained in this response (including the attached letter from PwC) constitutes Facebook's confidential business information and should be treated with the highest degree of confidentiality pursuant to 5 U.S.C. §§ 552(b)(3) & (b)(4) and 15 U.S.C. § 46(f).

As we have explained and as you noted in your letter, Facebook designed its Privacy Program to accomplish two primary objectives: (a) to address privacy risks related to the development, management, and use of new and existing products, and (b) to protect the information Facebook receives from or about users. As noted in the Assessment, Facebook has designed and implemented a broad range of "controls" that together form its robust Privacy Program—a program that we believe is industry leading. The Privacy Program achieves and effectuates Facebook's objectives and specifically includes "assessing impact on the Privacy Program from acquisitions." See 2017 Assessment at 8. In fact, for the relevant

reporting period, in 2015 Facebook implemented a new control oriented specifically to assessing and addressing risks relating to acquisitions:

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

See 2017 Assessment at 50 (Ref. H-6, Facebook's Control Activity). As you describe in your letter, and as reflected in Facebook's H-6 control, Facebook's assessment of the impact from acquisitions includes: (b)(4); (b)(3):6(f)

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

(b)(4); (b)(3):6(f) See *id.* at 50 (Ref. H-6, Facebook's Control Activity); see also *id.* at 32 (Ref. D-2, Facebook's Control Activity) (ongoing Privacy XFN review). Key members of the Privacy XFN team also review and update the privacy risk assessment. See *id.* at 24 (Ref. B-1, Facebook's Control Activity), 50 (Ref. H-5, Facebook's Control Activity). Consistent with your letter, Facebook's privacy risk assessments include, among other things, any identified material risks relating to acquisitions, including data sharing with and integration of acquired entities.

Your letter is correct that, (1) PwC tested Facebook's process for assessing risks presented by acquisitions, and (2) where Facebook's Privacy Program controls were applied to acquired entities, that application was subject to testing by PwC as part of the Assessment. (b)(4); (b)(3):6(f)

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

In addition, acquired entities that continue to operate independently after acquisition sometimes made use of Facebook's Privacy Program controls. When that happened, consistent with your letter, PwC tested the controls—(b)(4);

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

(b)(4); (b)(3):6(f) PwC concluded that Facebook's privacy controls were effective to protect the privacy of Facebook's covered information.

Finally, you are correct that, during the relevant time period, Facebook or one of its affiliates acquired (b)(4); (b)(3):6(f)

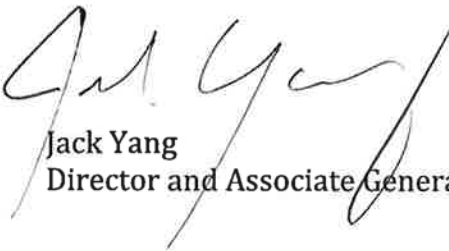
(b)(4); (b)(3):6(f) Because not all acquisitions by Facebook or one of its affiliates will affect Facebook's compliance obligations, not all acquisitions require notice to the Commission, pursuant to Section VIII of the Consent Order. However, we approach the notice obligation thoughtfully and have, out of an abundance of caution, often notified the Commission while our assessment of an acquisition is ongoing or its effect on compliance is not yet known. Not infrequently, such acquisitions ultimately do not affect compliance. During the relevant period, Facebook or one of its affiliates completed four additional acquisitions that did not impact Facebook's compliance obligations, and therefore Facebook did not notify the Commission: (b)(4);

(b)(4); (b)(3):6(f) Facebook acquired talent and technology associated with (b)(4); shut down its consumer-facing operations, and deleted all user data. During the same period, one of Facebook's affiliates acquired (b)(4); (b)(3):6(f) All three resulted in acquiring technology for and talent to an affiliate company, and did not impact Facebook's compliance obligations. In the future, we intend to continue taking a thoughtful approach to notifying the Commission.

* * *

Thank you for your time in reviewing our Assessment. Please let us know if you have any additional questions.

Sincerely,



Jack Yang
Director and Associate General Counsel, Head of Privacy



VIA EMAIL

Mr. Jack Yang
Director and Associate General Counsel, Privacy
Facebook, Inc.
1 Hacker Way
Menlo Park, CA 94025

July 28, 2017

Dear Jack:

This letter is a follow-up to our recent conversation regarding the letter Facebook received from the Federal Trade Commission ("FTC") dated June 1, 2017 in regards to our Biennial Independent Assessor's Report on Facebook's Privacy Program ("Assessment"), which was submitted for the period February 12, 2015 to February 11, 2017. Specifically, the FTC requested from Facebook "clarification regarding the scope of this Assessment with respect to Facebook's acquired entities and affiliates."

PwC has read your response letter to the FTC, dated July 28, 2017, and your description of the process to assess the impact of acquisitions on Facebook's Privacy Program (the "Privacy Program") is consistent with the description of the controls included in the *Facebook Privacy Program Overview* section of the report dated April 12, 2017. These controls were tested by PwC as described in the *Facebook's Privacy Program: Assertions, Control Activities and PwC's Tests Performed and Results* section of our Assessment.

Please let me know if there are additional questions.

Sincerely,

Joseph V. DiVito, Jr.
Principal

(b)(6)

PricewaterhouseCoopers LLP, 600 Grant St., Pittsburgh PA 15219
T: (412) 355 6000, www.pwc.com

Confidential

000119



UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Laura D. Koss, Esq.
Division of Enforcement
202-326-2890 (phone)
202-326-2558 (fax)

December 4, 2012

via U.S. and electronic mail (b)(6)

Mr. Edward Palmieri
Associate General Counsel, Privacy
Mr. Daniel Li
Product Counsel
Facebook, Inc.
1601 Willow Road
Menlo Park, CA 94025

Re: *In the Matter of Facebook, Inc.*, Docket No. C-4365

Dear Counsel:

Thank you for your email of November 21, 2012 apprising us of changes Facebook is proposing to make to its Data Use policy and terms. In addition, we have reviewed Facebook's 90-day compliance report dated November 13, 2012 ("compliance report"). The information you have provided to date raises several questions. Pursuant to Part IX of the Commission's Decision and Order ("Order"), we ask that Facebook address the issues described in sections A, B, and C below in writing by **December 18, 2012**. Additionally, based on our review of the compliance report, in section D we outline information Facebook should ensure is included in the 180-day Assessment ("Assessment") submitted in accordance with Part V of the Order.

A. Identification of Third-Party Professional to Conduct Assessments

Although Facebook signed the Order in November 2011, its compliance report states it has not yet selected the third-party professional it will propose to conduct the Assessment, as required by Part V. This raises concerns about Facebook's ability to submit a timely and complete Assessment as required. Please apprise us of the status of Facebook's selection of a proposed assessor.

B. Sharing With Affiliates

Facebook's proposed revisions to its Data Use Policy include a new section entitled

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

We are aware Facebook acquired Instagram in or about April 2012. In Facebook's SEC Prospectus filed May 18, 2012, Facebook stated that it "plan[s] to maintain Instagram's products as independent mobile applications to enhance our photos product offerings and to enable users to increase their levels of mobile engagement and photo sharing."

Please explain the precise nature of Facebook's relationship with Instagram. Your response should detail the following: (1) the legal relationship between Facebook and Instagram; (2) whether Facebook and Instagram ("the companies") have overlapping officers or directors; (3) whether the companies have overlapping personnel, including managers; (4) whether the companies have any integrated operations; (5) whether the companies have shared locations; (6) whether Instagram's finances are or will be included in Facebook's consolidated financial statements; (7) whether Facebook directs or participates in the development or implementation of Instagram's privacy policies; (8) whether any Instagram user information or content has been or will be transferred to Facebook; (9) whether any Instagram user information or content is stored or processed separately from Facebook user information; and (10) what control or influence Facebook has, if any, over Instagram's operations.

In addition, please explain whether or not you consider Instagram to be a "third party" as this term is defined under the Order and, if so, provide the basis for that determination. If Instagram is a third party, explain how, in Facebook's view, the sharing of information between the companies complies with the Order. If Instagram is not a third party for purposes of the Order, Facebook must ensure the Assessment comprehensively details the extent to which Facebook's privacy program (1) addresses the privacy risks related to Instagram products and services, and (2) protects the privacy and confidentiality of covered information, in accordance with Part IV of the Order.

C. Facebook Messages

Currently, Facebook's Data Use policy provides users with the ability to "control who can start a message thread with you using your 'How You Connect' settings." The proposed revisions, (b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f) Please explain how this proposed change complies with Part II of the Order, which triggers notice and affirmative express consent requirements (separate and apart from any "privacy policy," "data use policy," "statement of rights and responsibilities page," or other similar document) prior to any sharing of a user's nonpublic user information by Facebook with any third party which materially exceeds the restrictions imposed by a user's privacy settings.

D. Issues Raised by Facebook's Compliance Report

As you know, the Assessment must specifically demonstrate Facebook's compliance with the Order by addressing each of the items outlined in Part V of the Order.

In its compliance report, Facebook made several representations regarding the design and

implementation of its privacy program, indicating it “has taken extensive steps to establish, implement, and maintain the Privacy Program, which is documented in written policies and procedures.” Accordingly, Facebook should ensure the Assessment provides detailed information demonstrating the basis for each of its representations in this regard, including all documentation for the procedures and controls referenced in its compliance report. For example, the Assessment should address, at a minimum, the following:

1). Deleted User Information And Terminated Accounts (Part III)

Pursuant to Part III of the Order, Facebook must “implement procedures reasonably designed to ensure that covered information cannot be accessed by any third party from servers under [Facebook’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” Facebook’s compliance report states it has “comprehensive procedures for deleting information that has been deleted by users and ensuring that it cannot be accessed by third parties from servers under Facebook’s control after a reasonable period of time.” Please confirm this period does not exceed thirty days. In addition, the compliance report states Facebook has “implemented controls to ensure that any issues that arise with respect to data deletion are identified and addressed.” The Assessment should describe and evaluate the adequacy of those controls in detail.

2). Privacy Program (Part IV)

Part IV of the Order requires Facebook to “document in writing” the “content and implementation” of its comprehensive privacy program, which “shall contain controls and procedures appropriate to [Facebook’s] size and complexity, the nature and scope of [Facebook’s] activities, and the sensitivity of the covered information.” Facebook’s compliance report states that Facebook’s privacy program is “documented in written policies and procedures.” The Assessment should include copies of these written policies and procedures, in addition to providing a detailed evaluation of their effectiveness as specifically outlined in A through D of Part V.

(a) Designation of Employees (Part IV.A)

Part IV.A requires Facebook to designate an “employee or employees to coordinate and be responsible for the privacy program.” The Assessment should identify (by name, job position, and title) each member of Facebook’s “Privacy Cross-Functional Team.”

(b) Identification of Risks And Assessment of Safeguards (Part IV.B)

Part IV.B requires Facebook’s comprehensive privacy program to contain “controls and procedures,” including: (1) “the identification of reasonably foreseeable, material risks, both internal and external, that could result in the unauthorized collection, use, or disclosure of covered information” and (2) “an assessment of the sufficiency of any safeguards in place to

control these risks.”

Facebook’s compliance report states it has “documented its risk assessment and mapped its existing privacy controls to the GAPP framework.” In accordance with Part V, the Assessment should include this documentation and provide a detailed evaluation concerning Facebook’s risk assessment and privacy controls.

Additionally, Facebook states it has “identified key internal and external risks that could result in the unauthorized collection, use, or disclosure of covered information.” The Assessment should identify and describe these risks in detail.

Facebook also states its privacy program is “designed in part to identify changes that fall under the scope of Part II of the Order and to implement the disclosure and consent requirements . . . where applicable.” The compliance report further states that the specific policies and procedures it references “all contribute to identifying new or changed products or services that may trigger the disclosure and consent requirements of Part II of the Order.”

To demonstrate compliance with the Order, Facebook must ensure the Assessment identifies all risks that could result in the unauthorized collection, use, or disclosure of information and explains how Facebook’s safeguards sufficiently control these risks. Specifically, the Assessment should detail every new or changed product or service, including, but not limited to, products and services relating to Facebook’s acquisition of Instagram, Facebook’s partnership with Datalogix and other third parties, Facebook’s facial recognition/tag suggestion feature, changes in Facebook’s messages mechanism, and changes to the ability to search for Facebook users within the Facebook interface. For each new or changed product or service, the Assessment should explain whether and why Facebook has, or has not, implemented the disclosure and consent requirements required by Part II of the Order.

(c) Controls And Procedures to Address Privacy Risks (Part IV.C)

Part IV.C requires Facebook to document 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.”

Facebook’s compliance report states that Facebook has performed “granular mapping of its existing privacy controls to the GAPP framework,” that it has “assessed each GAPP criteria to determine if the controls in place adequately controlled for the associated risks,” that it has “identified certain controls that had room for enhancement,” and that it has “implemented remediation plans with respect to those controls.” The compliance report further states Facebook has “documentation of a mapping of Facebook’s controls to the GAPP framework, along with the status of each control.” Facebook should ensure the Assessment includes the aforementioned documentation and provides a list of each of Facebook’s existing privacy controls, indicating the specific controls for which Facebook implemented “remediation steps” (as noted in the compliance report) and explaining the justification for those modifications.

In addition, Facebook states it has designated an "owner" for each of the controls and procedures included in its privacy program, to "ensure that the effectiveness of its controls and procedures" are regularly monitored. The Assessment should identify by name, job position and title every person who has been designated an "owner" and, for each, list the specific controls/procedures the individual is charged with monitoring.

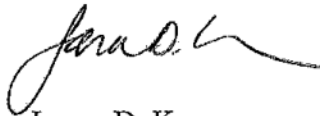
* * * * *

The Commission staff reserves the right to request additional information and to pursue other avenues of inquiry as we may deem appropriate.

As indicated in the instruction sheet previously enclosed with my letter of August 29th, compliance reports filed pursuant to an administrative order and supplemental materials filed in connection with the reports become public records unless a request for confidentiality is granted. *See* 16 C.F.R. §4.9(b)(7) & (c). For your convenience, we have enclosed another copy of this instruction sheet, which provides detailed instructions on requesting confidentiality.

Your prompt cooperation in this matter is appreciated. If you have any questions, please do not hesitate to contact me at (202) 326-2890 or Reenah Kim at (202) 326-2272.

Sincerely yours,



Laura D. Koss
Reenah L. Kim
Attorneys

Enclosure



December 18, 2012

sent via email to lkoss@ftc.gov and rkim1@ftc.gov

Laura D. Koss
Division of Enforcement
Federal Trade Commission
Washington, DC 20580

Re: *In the Matter of Facebook, Inc.*, Docket No. C-4365

Dear Laura,

I write in response to your letter dated December 4, 2012 requesting various categories of information from Facebook. We provide the below information to address your questions and look forward to submitting our first independent assessment (“Assessment”) next year.¹

Material contained in this response constitutes Facebook confidential business information, and we ask that it be treated with the highest degree of confidentiality pursuant to 5 U.S.C. 522(b)(3) & (b)(4) and 15 U.S.C. 46(f).

A. Identification of Third-Party Professional to Conduct Assessments

You first asked Facebook to identify whom it has chosen to perform the Assessment required under Part V of the Decision and Order, served on Facebook on August 15, 2012 (“Order”). Facebook has selected PricewaterhouseCoopers LLP (“PwC”) to conduct the Assessment.

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

[Redacted]

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

[Redacted]

¹ Some of the information requested in your letter appears to concern matters outside the scope of Facebook’s obligations under the Order and the recent compliance report that Facebook filed pursuant to Part IX of the Order. While Facebook is pleased to offer the information contained herein in the spirit of cooperation, we do so without waiving any rights or defenses.



B. Instagram Acquisition

You next requested information about the nature of Facebook's relationship with Instagram, LLC.

Facebook closed its acquisition of Instagram in September of this year, after the Commission reviewed the transaction under the Hart-Scott-Rodino Antitrust Improvements Act. Following the acquisition, Instagram became a wholly owned subsidiary of Facebook. While Facebook operates Instagram as a separate brand with distinct products and services, the two companies are affiliates and have overlapping officers, directors and personnel, as well as integrated business operations (which will continue to be further integrated over time). Facebook shares office space with Instagram, accounts for Instagram in its consolidated financial statements, and has direct control over Instagram's business operations.

We continue to evaluate ways where we may integrate Instagram and Facebook, to help Instagram function more efficiently as part of Facebook. Sharing information between the two groups allows us to perform functions such as fighting spam more effectively, detecting system and reliability problems more quickly, enhancing the safety and security of our users, and building better features and products.

Instagram is part of Facebook, not a separate entity that constitutes a "third party" for the purposes of the Order. As a part of Facebook, Instagram's operations will be covered as part of the Assessment.

C. Facebook Messages ("Messages")

You next requested information related to Facebook Messages. Messages is a central place to communicate with people on and off Facebook. For example, people may send messages to their friends or groups of friends. In your letter, you asked whether recently announced changes to the Messages product implicate Part II of the Order, which requires that Facebook provide notice and obtain affirmative express consent prior to sharing a user's nonpublic user information with a third party in a manner that materially exceeds the restrictions imposed by the user's privacy setting(s).² The settings for Messages do not implicate Part II of the Order because they do not involve the sharing of nonpublic user information. Rather, the settings only affect the ability of others to send messages to a Facebook user.

Nonetheless, we would like to take this opportunity to provide the context for recent changes to the portion of Facebook's Data Use Policy identified in your letter. Facebook's existing message filtering tools offer users rudimentary control over the flow of communications through Messages. Specifically, the controls currently require users to choose between allowing messages from "everyone," including individuals with no connection to them, or restricting messages to either "friends" or "friends of friends," thereby potentially blocking messages they might want to receive, such as a message from a

² "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." Order at Part II.



new coworker, someone who already has their contact information but isn't a friend on Facebook, or a long-lost friend with whom the user shares no friends in common.

Facebook's new messaging controls attempt to address these limitations by applying advanced logic that examines a wider range of factors to separate and organize a user's messages into appropriate folders. These new filters aim to provide users with smarter tools that help them focus on important messages first. Even when these new tools are in place, users will continue to have the ability to block messages from specific users.

Facebook is, of course, going to great lengths to explain these new tools to users. In addition to the Data Use Policy changes mentioned in your letter, Facebook will also present users with in-context education as the new messaging filters are rolled out. This information will explain that the old tools have been retired and that new filters are now in operation.

D. Third-Party Assessment

Your letter concludes with a section identifying several categories of information that you request Facebook include as part of the Assessment required under Part V of the Order.

As noted in Part A of this letter, Facebook has retained PwC — “a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession” — to conduct the Assessment required under the Order. The Order, in turn, specifies the topics and information that must be included in the Assessment. We will certainly share a copy of your letter and our reply with the third-party assessor, and we expect that they will be guided by generally accepted procedures and standards and the terms of the Order in determining what to include in the Assessment.

* * *

We look forward to continuing our dialogue with you regarding our compliance with the Order. Please do not hesitate to contact me should you have any additional questions.

Sincerely,

Edward Palmieri
Associate General Counsel, Privacy



UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

James A. Kohm
Associate Director
Division of Enforcement

January 8, 2013

via U.S. and electronic mail (b)(6)

Mr. Edward Palmieri
Associate General Counsel, Privacy
Mr. Daniel Li
Product Counsel
Facebook, Inc.
1601 Willow Road
Menlo Park, CA 94025

Re: *In the Matter of Facebook, Inc., Docket No. C-4365*

Dear Counsel:

Your December 18, 2012 letter apprises us that Facebook has chosen Pricewaterhouse Coopers LLP ("PWC") to conduct the Assessments required under Part V of the Commission's Decision and Order ("Order").

Under Part V of the Order, the Enforcement's Associate Director must approve "persons selected to conduct the Assessments." I approve PWC to conduct the initial and biennial Assessments and reports required under Part V. As in all cases, I reserve the right to retract this approval if PWC does not prove to be a qualified, objective, independent third-party professional or if PWC evidences a failure to effectively conduct its responsibilities as required by the Order.

Sincerely,

James A. Kohm
Associate Director
Division of Enforcement



UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
600 Pennsylvania Avenue NW
WASHINGTON, D.C. 20580

Reenah L. Kim
Bureau of Consumer Protection
Division of Enforcement, Mailstop M-8102B
Direct Dial: (202) 326-2272

June 26, 2013

via Federal Express and electronic mail (b)(6)

Mr. Edward Palmieri
Associate General Counsel, Privacy
Mr. Daniel Li
Product Counsel
Facebook, Inc.
1601 Willow Road
Menlo Park, CA 94025

Re: *In the Matter of Facebook, Inc.*, Docket No. C-4365

Dear Counsel:

A June 21, 2013 blog post by Facebook Security described the recent discovery of a “bug that may have allowed some of a person’s contact information (email or phone number) to be accessed by people who either had some contact information about that person or some connection to them” when users downloaded an archive of their Facebook account through the “Download Your Information (DYI)” tool. Pursuant to Part IX of the Federal Trade Commission’s Decision and Order (“Order”), please provide a true and accurate written report that responds to the following within ten (10) days:

- 1) Set forth in detail exactly what happened, including but not limited to explaining:
 - (a) The types of covered information Facebook shared as a result of the “bug.”
 - (b) The method and means by which such covered information was shared;
 - (c) The time period during which such covered information was shared; and
 - (d) Whether the users whose covered information was shared as a result of the “bug” had granted permission in advance for Facebook to share this particular information with the individual(s) who received it.
- 2) Specify how many downloaded DYI archives included covered information shared as a result of the “bug.”

- 3) Specify how many Facebook users had their covered information shared as a result of the "bug."
- 4) Specify how many telephone numbers were shared as a result of the "bug."

- 5) Specify how many email addresses were shared as a result of the "bug."
- 6) Of the user telephone numbers shared as a result of the "bug," specify how many were shared in a manner that differed from the restrictions imposed by users' privacy setting(s).
- 7) For the number of user telephone numbers identified in response to question 6, specify how many were instances in which Facebook, prior to the sharing of such information, (a) clearly and prominently disclosed: (i) that the telephone numbers would be disclosed to third parties; (ii) the identities or specific categories of such third parties; and (iii) that such sharing would exceed the restrictions imposed by the privacy setting(s) in effect for the user, and (b) obtained the user's affirmative express consent.
- 8) Of the user email addresses shared as a result of the "bug," specify how many were shared in a manner that differed from the restrictions imposed by users' privacy setting(s).
- 9) For the number of user email addresses identified in response to question 8, specify how many were instances in which Facebook, prior to the sharing of such information, (a) clearly and prominently disclosed: (i) that the email addresses would be disclosed to third parties; (ii) the identities or specific categories of such third parties; and (iii) that such sharing would exceed the restrictions imposed by the privacy setting(s) in effect for the user, and (b) obtained the user's affirmative express consent.

Please have a responsible corporate officer or manager of Facebook certify under penalty of perjury that the report and information produced or identified in response to this demand letter are complete and accurate, and that the report and information represent all information responsive to this letter. Please send your responses via overnight courier (e.g., FedEx, UPS) to:

Associate Director
Division of Enforcement
Federal Trade Commission
600 Pennsylvania Ave. NW
Mailstop M-8102B
Washington, DC 20580

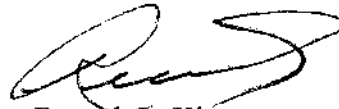
Re: *In the Matter of Facebook, Inc.*, Docket No. C-4365

June 26, 2013
page 3

In lieu of overnight courier, you may send your response by first-class mail, but only if you contemporaneously send an electronic copy to the Commission at DEBrief@ftc.gov, with a courtesy copy to us at lkoss@ftc.gov and rkim1@ftc.gov.

If you have any questions, please do not hesitate to contact us at 202-326-2272 (Reenah Kim) or 202-326-2890 (Laura Koss).

Sincerely yours,

A handwritten signature in black ink, appearing to read 'Reenah L. Kim', written in a cursive style.

Reenah L. Kim
Laura D. Koss
Attorneys



United States of America
FEDERAL TRADE COMMISSION
Washington, D.C. 20580

Laura D. Koss
Bureau of Consumer Protection
Division of Enforcement

600 Pennsylvania Ave., NW
Mailstop CC-9528
Washington, DC 20580

(202) 326-2890
Lkoss@ftc.gov

April 2, 2015

Mr. Edward Palmieri
Associate General Counsel, Privacy
Facebook, Inc.
1155 F. Street, NW Suite 475
Washington, DC 20004

VIA EMAIL

Re: *In the Matter of Facebook, Inc.*, FTC Docket No. C-4365

Dear Mr. Palmieri:

I am writing to remind Facebook (“the Company”) of its compliance obligations under Parts VIII, IV, V, and I of the Order in the above-referenced matter when the Company experiences corporate changes such as acquisitions.

First, Part VIII requires the Company to notify the Commission within fourteen days of “any change in Respondent that may affect compliance obligations arising under [the] order, including, but not limited to, . . . the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order.” (emphasis added). Whenever a corporate change such as an acquisition may affect the design and/or implementation of the Company’s privacy program, the Company must notify the Commission.

Second, Part IV provides that the reasonableness of the Company’s privacy program’s design and operation depends on the Company’s size and complexity, the nature and scope of its activities, and the sensitivity of the Covered Information. Corporate changes such as acquisitions are likely to affect several, if not all, of these factors. The Company, therefore, has an obligation to evaluate the appropriateness of its privacy program in light of any such changes.

Third, Part V requires the Company to obtain periodic Assessments, which address the ongoing effectiveness of the Company’s privacy program. To comply with Part V, the Assessment must address the safeguards required by Part IV, which may change in response to corporate changes like acquisitions. The Assessment must also explain how these safeguards are appropriate to the Company’s changing size and complexity, the nature and scope of its

activities, and the sensitivity of the Covered Information. Prompt and thorough communication with the Assessor about corporate changes such as acquisitions that may affect compliance obligations should facilitate the assessment of the Company's privacy program.

Finally, Part I provides that the Company shall not misrepresent the extent to which it maintains the privacy or security of Covered Information. The Company has an obligation to ensure that, as of the date of acquisition, the representations of companies it acquires are truthful and non-misleading.

Please do not hesitate to contact me if you have any questions.

Sincerely,

A handwritten signature in black ink, appearing to read "Laura D. Koss". The signature is fluid and cursive, with the first name being the most prominent.

Laura D. Koss

cc: PricewaterhouseCoopers



UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Division of Enforcement
Bureau of Consumer Protection

August 29, 2012

Via Federal Express

Facebook, Inc.
c/o Theodore W. Ullyot
1601 Willow Road
Menlo Park, California

**Re: In the Matter of Facebook, Inc.
FTC Docket No. C-4365**

Dear Mr. Ullyot:

I am writing to introduce myself as the staff attorney assigned to monitor compliance with the Commission's Decision and Order ("Order") in this matter. As you know, the Order requires Facebook, Inc. ("Facebook") to report on its compliance with the Order within 90 days after service of the Order. Because the Order was served on August 15, 2012, the report is due on November 13, 2012.

The compliance report should describe in detail the modifications made to Facebook's privacy and other business practices to bring it into compliance with the Order. Follow the outline of the Order, paragraph by paragraph, explaining exactly how Facebook has complied with each provision of the Order. At a minimum, the report should include a description of:

1. modifications made to Facebook's privacy and business practices to ensure that it will not misrepresent the extent to which it maintains and protects the privacy and security of any covered information (as defined in the Order);
2. modifications made to Facebook's privacy and business practices to ensure that prior to any sharing of a Facebook's user's nonpublic user information with a third party it will make the disclosures required under section II.A of the Order and will obtain the Facebook user's affirmative consent, if such sharing materially exceeds the restrictions imposed by a Facebook user's privacy settings;
3. modifications made to Facebook's privacy and business practices to ensure that

covered information cannot be accessed by any third party from servers under Facebook's control after a reasonable period of time (not to exceed 30 days) from the time that the Facebook user has deleted such information or deleted or terminated his or her account; and

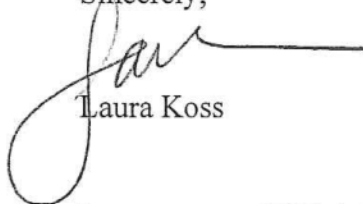
4. Facebook's comprehensive privacy program, including the controls and procedures used to (i) address privacy risks related to the development and management of new and existing products and services for consumers, and (ii) protect the privacy and confidentiality of covered information.

The foregoing description should not be construed as limiting the information that may be required to demonstrate full compliance with the Order.

Additionally, Section V of the Order requires Facebook to obtain an initial and thereafter biennial Assessments from a third-party professional. Please note that, per Section V.D of the Order, the Assessments must contain the following certification: "that [Facebook's] 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."

Please note that Facebook must submit the compliance report (and any other formal submission required by the Order) to the Enforcement Division, addressed to the Associate Director of Enforcement rather than to me. Enclosed is an instruction sheet that gives important additional guidance on this and other frequently asked questions. Also enclosed, for your convenience, is a form for the Acknowledgments of receipt of the Order that are required by the Order. If you have additional questions, you are welcome to contact me at (202) 326-2890 or at lkoss@ftc.gov.

Sincerely,



Laura Koss

Enclosures: Instructions For Submissions Pursuant to an FTC Administrative Order

CC: Debrief@ftc.gov

Instructions for Submissions Pursuant to an FTC Administrative Order

The staff of the Division of Enforcement provides this instruction sheet to answer frequently asked questions about compliance reports and other submissions. If at any time we supersede these general instructions with more specific instructions concerning your order, we will do so in writing.

1. Contact the Enforcement Division First: After the Commission issued the order against you, the Bureau of Consumer Protection transferred this matter from the Division or Region that negotiated or litigated the order to us in the Enforcement Division. We assigned a staff attorney to monitor your compliance with the Order.

2. Comply Promptly: We expect all respondents to come into compliance with consent (i.e., agreed or non-litigated) orders before they are served and with all other orders when they become final. There is no "grace" or other transition period. For example, unless the order expressly allows for the continued sale of pre-existing inventory or other such run-out, cease the sale of products or services with violative claims immediately. Your obligation to comply is never deferred pending submission of a compliance report, upon submission of a report that does not evidence full compliance with the order, or by any other action or inaction by you.

3. File Timely: The order requires that you submit a compliance report by a deadline. We may discover deficiencies and call them to your attention if you submit your report well before the deadline. If you request an extension of time to submit the report, you should do so in writing and show good cause for an extension, to the Associate Director of Enforcement. An extension of time to submit the report will not otherwise relieve your obligation to comply with the order.

4. Report With Specificity: Your compliance report must, at a minimum, contain a detailed description of how you have complied with each provision of the order. It is not sufficient merely to state in general terms that you are in compliance.

5. Report On Related Activities: Corporate respondents must report on the relevant activities of their subsidiaries and divisions, as well as their independent contractors and joint ventures with other firms. Individual respondents must report on the activities of those enterprises that they own or control or in which they participate, even if such enterprises are not named in the order.

6. Identify Exhibits: Support your compliance report with samples or other evidence that you submit along with the report as exhibits. Number each exhibit, identify each in the text of the report, and explain how each exhibit shows compliance with the order. If an exhibit cannot be duplicated for submission, then contact the assigned staff attorney for instructions. Be prepared to submit the original to the Associate Director of Enforcement and to note that fact in the cover letter and on each placeholder in the parallel submission to the Secretary. (See below: Submit Your Compliance Report Properly; and Request Confidential Treatment, If Appropriate).

7. Affirm All Submissions: All submissions should be notarized and sworn under oath by the individual respondent or by an authorized representative on behalf of the corporate respondent. Alternatively, comply with 28 U.S.C. § 1746, such as by concluding the submission: "I affirm under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: _____" and supplying the date, signatory's full name, title (if applicable), and signature. If multiple respondents file a single compliance report, each respondent must execute an affirmation.

8. Send All Submissions to the Enforcement Division: Compliance reports pursuant to the order and any supplemental materials, as well as any other submission, such as pursuant to a staff request or not pursuant to the order but otherwise involving this matter, all should be sent to the Enforcement Division.

a. To the Assigned Enforcement Attorney: Send questions or any other routine correspondence only to the assigned staff attorney.

b. To the Associate Director of Enforcement: Send formal submissions required by the Order, such as the compliance report, directly to the Associate Director of Enforcement. Send one copy either via email to DEbrief@ftc.gov or via a delivery service to: Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. Do not send your formal submission to the assigned staff attorney unless a courtesy copy is specifically requested, and even then any formal submission must be sent to the Associate Director.

c. Steps to Ensure Prompt Receipt: Begin the subject line of all email and paper submissions: (name of your case and its C or D #). For paper submissions use a delivery service such as Federal Express or UPS, but not the U.S. Postal Service. Until further specified by staff, electronic submission should be in Adobe portable document format, which is a PDF. If you have questions about submissions to the Enforcement Division, contact the assigned staff attorney.

9. Send Some Submissions to the Secretary of the Commission: Compliance reports pursuant to the administrative order and supplemental materials, if any, should also be sent to the Secretary, where they will be placed on the public record (unless confidentiality is requested and granted as discussed below). Send the original, two paper copies, and an electronic copy on CD or DVD in Adobe portable document format to: Secretary, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. *See* 16 C.F.R. § 4.2 for additional requirements as to form and filing.

10. Request Confidential Treatment, If Appropriate: Compliance reports filed pursuant to an administrative order and supplemental materials filed in connection with the reports become public records unless a request for confidentiality is granted. *See* 16 C.F.R. § 4.9(b)(7) & (c).

a. How to Request Confidentiality: At the time of submission, you as the filing party may request confidential treatment for the submission in whole or in part. To be a valid request, a request for confidentiality may not be general in nature and must: (a) identify the specific part of the submission for which confidentiality is claimed; (b) provide a detailed justification as to

why the material should be kept confidential; and (c) include a second version of the submission where the material claimed to be confidential is redacted. Do not simply delete the proposed redacted language; instead black it out, replace it with the word "redacted," or otherwise preserve the formatting of the original document.

b. Common Grounds for Confidentiality: Confidential commercial or financial information is exempt from public disclosure if its disclosure is likely to cause substantial competitive harm to you. *See* 15 U.S.C. § 46(f); 5 U.S.C. § 552(b)(4); 16 C.F.R. § 4.10(a)(2). Personnel, medical, and similar files may be exempt from public disclosure if disclosure would constitute a clearly unwarranted invasion of personal privacy. *See* 5 U.S.C. § 552(b)(6); 16 C.F.R. § 4.10(a)(4).

c. Results of a Confidentiality Request: The Commission's Office of General Counsel decides requests for confidentiality. If the General Counsel deems a document you submitted to be confidential, the Commission will not disclose such document without affording you 10 days notice of its intent to do so, except as provided in 15 U.S.C. §§ 46(f) and 57b-2, and the applicable Commission Rules. If the General Counsel denies your request for confidential treatment of any document, the document will be placed on the public record no sooner than 10 days after you receive written notification that your request for confidential treatment was denied.

11. Expect No Notice of Noncompliance: We rarely give compliance advice and sometimes do not alert respondents if we plan to recommend that the Commission take action. The Commission is not obligated to notify you before instituting legal proceedings.

12. Draw No Inference of Compliance: Absent express, written confirmation to you from the Associate Director of Enforcement, you should not construe silence about a reported practice, advice on how to comply, or any other action or inaction by the staff to mean that you are in compliance with the order. We may request additional information or pursue noncompliance at any time allowed by the order.

13. You Face Penalties for Noncompliance: Any person or business who "violates an order of the Commission after it has become final, and while such order is in effect, shall forfeit and pay to the United States a civil penalty," which as of 2011 was up to \$16,000 for each violation. *See* 15 U.S.C. § 45(l); 16 C.F.R. § 2.41(c); *see also* 28 U.S.C. § 2461; 16 C.F.R. § 1.98; (periodically adjusting the penalty amount for inflation). Federal district courts are also empowered to grant mandatory injunctions and other equitable relief, including consumer refunds, corrective advertising, and disgorgement of profits. *See* 15 U.S.C. § 45(l).

From: Stephanie Kretschmer
Sent: 20 Jun 2011 23:45:42 +0000
To: JDL
Subject: Call with Elliot Schrage

Hi Jon,

Elliot tried your cell but it sounds like you two didn't connect today. Are you available at 9:30am PST tomorrow? Or let me know what times you can talk and I'll do my best to make Elliot available then.

Thanks!

Stephanie M. Kretschmer
Executive Assistant to Elliot Schrage | Facebook
VP Global Communications, Marketing & Public Policy

(b)(6)

From: Elliot Schrage
Sent: 22 Jun 2011 01:23:25 +0000
To: JDL
Cc: Joel Kaplan
Subject: electronic introduction

Jon,

As promised, I want to introduce you to Joel Kaplan, who now heads our DC policy efforts. He's the right person to coordinate a briefing for your team on our new service updates scheduled to be announced in the next few weeks.

Best,

Elliot

--

Elliot Schrage | VP Communications, Marketing and Public Policy

Facebook | (b)(6)

(b)(6)

Mailing Address: 1601 S. California Avenue, Palo Alto, CA 94304

From: Elliot Schrage
Sent: 21 Jun 2011 23:44:03 +0000
To: JDL
Subject: Re: just tried to reach you

Just checking

--
Elliot Schrage | VP Communications, Marketing and Public Policy
Facebook (b)(6)
(b)(6)
Mailing Address: 1601 S. California Avenue, Palo Alto, CA 94304

On 6/21/11 4:25 PM, "JDL" <JDL@ftc.gov> wrote:

>I will call you in two mins.

>

>-----Original Message-----

>From: Elliot Schrage [mailto:(b)(6)]

>Sent: Tuesday, June 21, 2011 7:09 PM

>To: JDL

>Subject: just tried to reach you

>

>I am at (b)(6) the gods are conspiring against us

>--

>Elliot Schrage | VP Communications, Marketing and Public Policy

>Facebook (b)(6)

(b)(6)

>Mailing Address: 1601 S. California Avenue, Palo Alto, CA 94304

>

>

>

>

From: Joel Kaplan
Sent: 23 Aug 2011 20:03:19 +0000
To: Lupovitz, Joni;JDL
Subject: Re: Thank you
Attachments: Easier_To_Share_With_Who_You_Want_FINAL[1].docx

Thanks Joni. As promised, here's a copy of the blog post and screenshots we put out today. Changes started rolling out Thurs. Hope everyone at the FTC is okay and stayed out of harm's way today. All the best—Joel

From: "Lupovitz, Joni" <JLUPOVITZ@ftc.gov>
Date: Tue, 23 Aug 2011 11:02:11 -0400
To: Joel Kaplan <(b)(6)> JDL <JDL@ftc.gov>
Subject: Re: Thank you

Thanks for the heads' up & good luck--
Best,
Joni

Joni Lupovitz
Chief of Staff
Office of Chairman Jon Leibowitz
Federal Trade Commission
202-326-3743

From: Joel Kaplan [mailto:(b)(6)]
Sent: Monday, August 22, 2011 04:24 PM
To: JDL
Cc: Lupovitz, Joni
Subject: Re: Thank you

Chairman:

Hope your summer is going well. I wanted to give you and Joni a heads-up that we are planning on announcing tomorrow the privacy enhancements and product changes we briefed you and your team on last month. We are going out with a blog post explaining the changes at 11:00 am Pacific time, and will actually begin rolling them out on the site on Thursday. I will shoot you a copy of the blog post and some accompanying "screen shots" of the changes tomorrow. Please don't hesitate to email or call (b)(6) if you have any questions, either before the announcement or anytime after.

Thanks again for your time last month. Best—Joel

From: JDL <JDL@ftc.gov>
Date: Sat, 16 Jul 2011 14:46:55 -0400
To: Joel Kaplan <(b)(6)> "Lupovitz, Joni" <JLUPOVITZ@ftc.gov>
Subject: Re: Thank you

Hi Joel,

Thanks so much for coming in and facilitating a really interesting presentation. It seems like you are enjoying yourself at Facebook, and Facebook is extraordinarily lucky to have you on board.

Looking forward to working together & best,

Jon

Sent from JDL Blackberry

From: Joel Kaplan [mailto:(b)(6)]
Sent: Friday, July 15, 2011 09:53 PM
To: JDL; Lupovitz, Joni
Subject: Thank you

Chairman--

Didn't want the week to pass without thanking you and your team for the opportunity to visit with you earlier this week about upcoming changes to our product. I know how much you have on your plate, and so really appreciated the chance to come in and walk you and your team through the changes and why they are being made. We are excited about the changes, and hopefully the influence of the December privacy report was evident in the presentation. I will be sure to let Joni know when we are prepared to announce the changes. In the meantime, please let me know if you have any questions.

Thanks again, and all the best--

Joel

Making It Easier to Share with Who You Want

Today we're announcing a bunch of improvements that make it easier to share posts, photos, tags and other content across Facebook with exactly the people you want. You have told us that "who can see this?" could be clearer across the board, so we have made changes to make this more visual and straightforward. The main change is moving most of your controls from a settings page to being inline, right next to the posts, photos and tags they affect. Plus there are several other updates here that will make it easier to understand who can see your stuff (or your friends') in any context. Here's what's coming up, organized around two areas: what shows up on your profile, and what happens when you share something new.

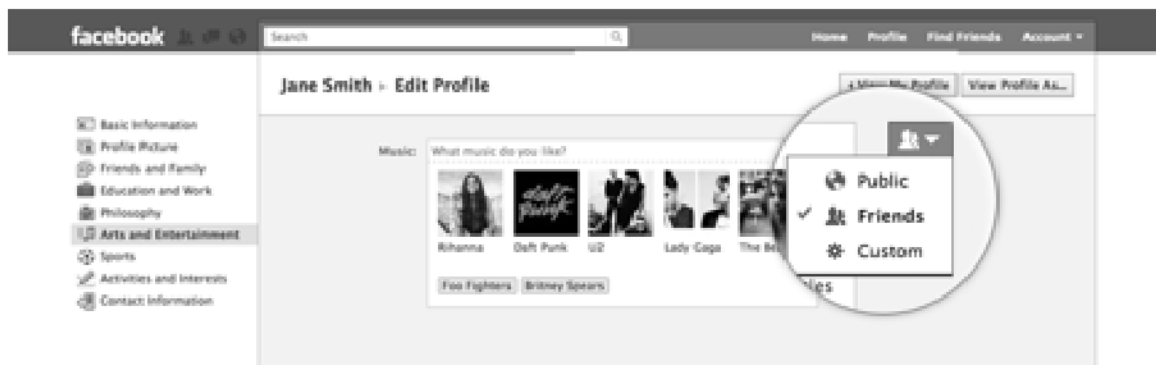
1. On Your Profile

Your profile should feel like your home on the web -- you should never feel like stuff appears there that you don't want, and you should never wonder who sees what's there. The profile is getting some new tools that give you clearer, more consistent controls over how photos and posts get added to it, and who can see everything that lives there.

Inline profile controls

Before: most of the settings for stuff on your profile were a few clicks away on a series of settings pages.

Going forward: content on your profile, from your hometown to your latest photo album, will appear next to an icon and a drop-down menu. This inline menu lets you know who can see this part of your profile, and you can change it with one click.



A side benefit of moving most settings to inline controls is a much shorter and simpler Settings page. A bunch of settings that were there previously have been moved directly inline, and a handful have been replaced or removed. (You can find more detail on the profile settings here: <http://www.facebook.com/about/control>)

Profile tag review

Before: photos you were tagged in would show up on your profile as soon as you were tagged. One of the top requests we've heard is for the ability to approve these tags before they show up on your profile.

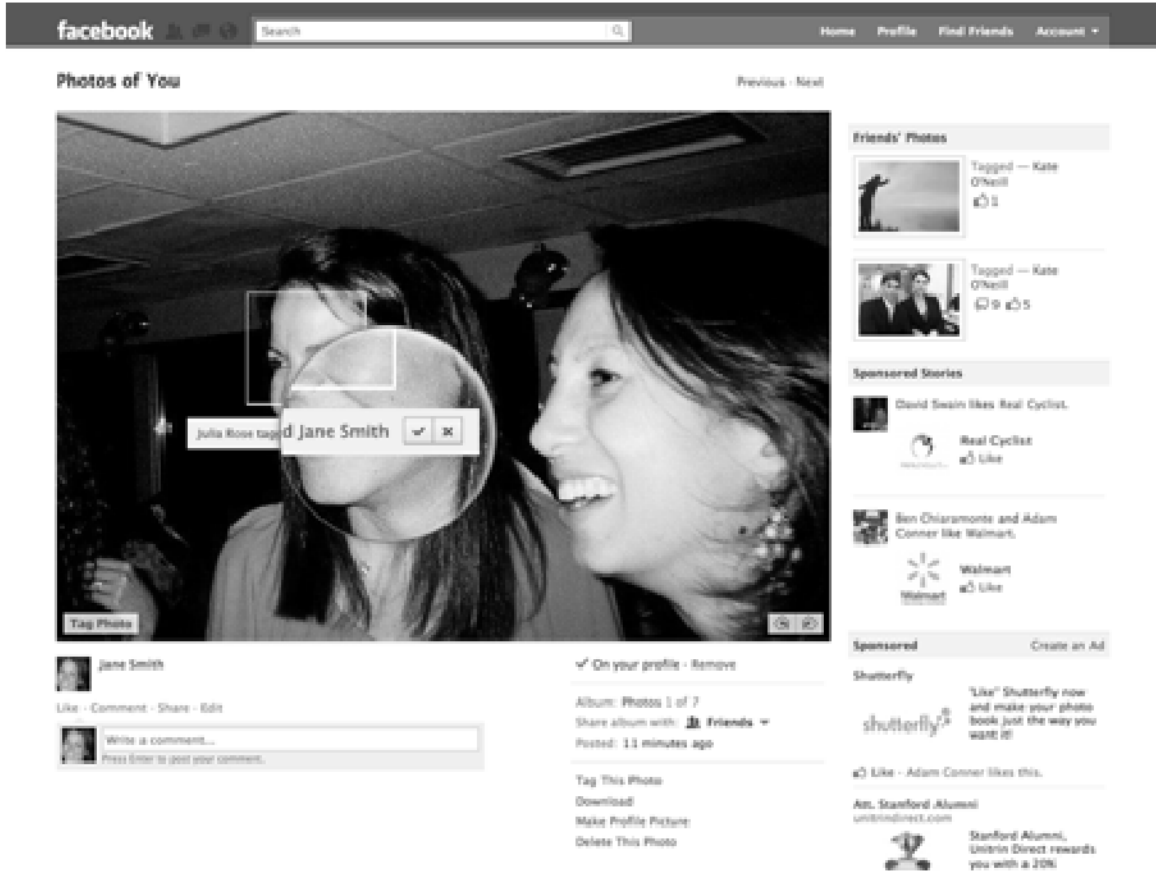
Going forward: you can choose to use the new tool to approve or reject any photo or post you are tagged in before it's visible to anyone else on your profile.



Content tag review

Before: anyone who could see your photos or posts could add tags to them.

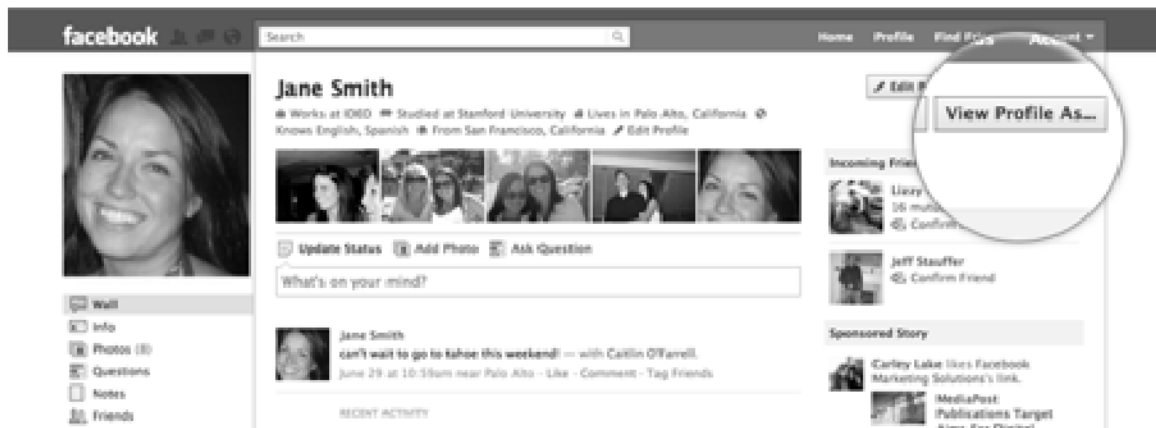
Going forward: you have the option to review and approve or reject any tag someone tries to add to your photos and posts.



View Profile As...

Before: we heard you wanted to know what your profile looked like to others, but the tool for doing this was behind the scenes.

Going forward: this tool is now on the top of your profile where it's easier to access.



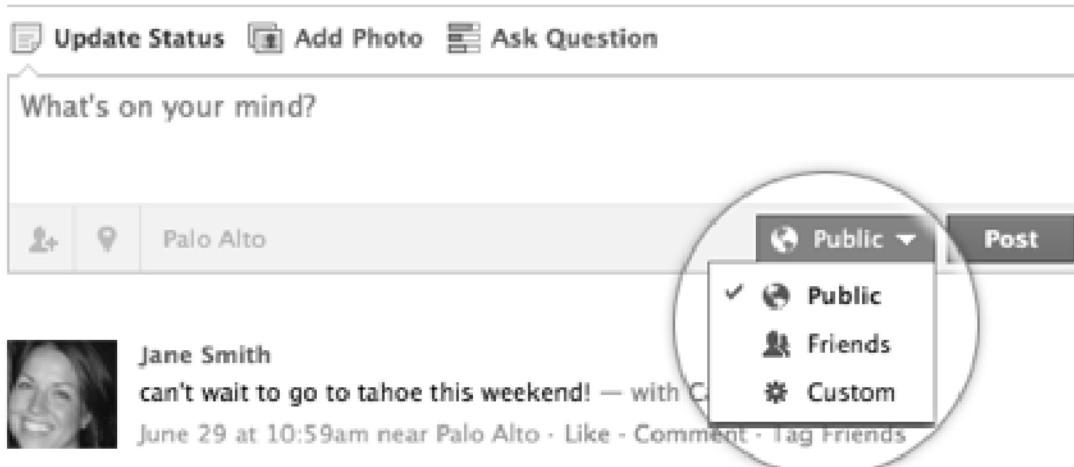
2. When You Share

In addition to the profile changes, it will now be more visually straightforward to understand and control who can see your posts at the time you share them. We're also broadening the functionality of the sharing tool: now if you want to make your posts more expressive, we've made it simple to add location and tag the people you're with.

Inline controls

Before: controls for who could see you stuff on Facebook lived on a settings page a few clicks away.

Going forward: the control for who can see each post will be right inline. For each audience, there is now a unique icon and label to help make it easier to understand and decide who you're sharing with. Also, when you tag someone, the audience label will automatically update to show that the person tagged and their friends can see the post.



This dropdown menu will be expanding over time to include smaller groups of people you may want to share with, like co-workers, Friend Lists you've created, and Groups you're a member of. These will make it easy to quickly select exactly the audience you want for any post.

If you're posting to Facebook from a phone or app that does not yet support inline controls, your setting will be the same as it is today. You can change this with a new setting available on your privacy settings page. (For a guided tour of these new controls, go here: <http://www.facebook.com/about/sharing>)

Word change: "Everyone" to "Public"

Before: you had the option to share a post with Everyone, which meant that anyone on the internet might be able to see it.

Going forward: we are changing the name of this label from Everyone to Public so that the control is more descriptive of the behavior: anyone may see it, but not everyone will see it. This is just to make the setting more clear, and it's just a language change.

Change your mind after you post?

Before: once you posted a status update, you couldn't change who could see it.

Going forward: now you'll be able to change who can see any post after the fact.

If you accidentally posted something to the wrong group, or changed your mind, you can adjust it with the inline control at any time.

Tag who you're with, or what you want to talk about

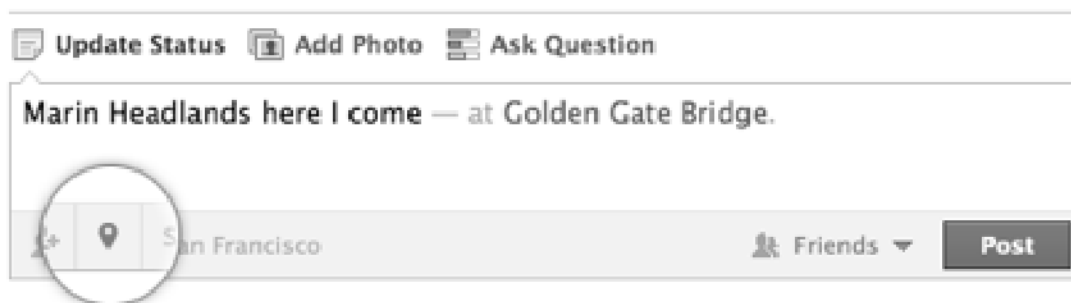
Before: you could only tag someone if you were friends with them, and you could only tag a Page if you had liked it. This felt broken or awkward if you had a photo album of co-workers and had to become Facebook friends to tag them in the photos.

Going forward: you can add tags of your friends or anyone else on Facebook. If you are ever tagged by a non-friend, it won't appear on your profile unless you review and approve the post.

Tag locations in posts

Before: you could only "check in" to locations using the Places feature on a smart phone.

Going forward: now you can add location to anything. Lots of people use Facebook to talk about where they are, have been or want to go. Now you can add location from anywhere, regardless of what device you are using, or whether it is a status update, photo or Wall post. Of course, you can always choose not to add location at all.



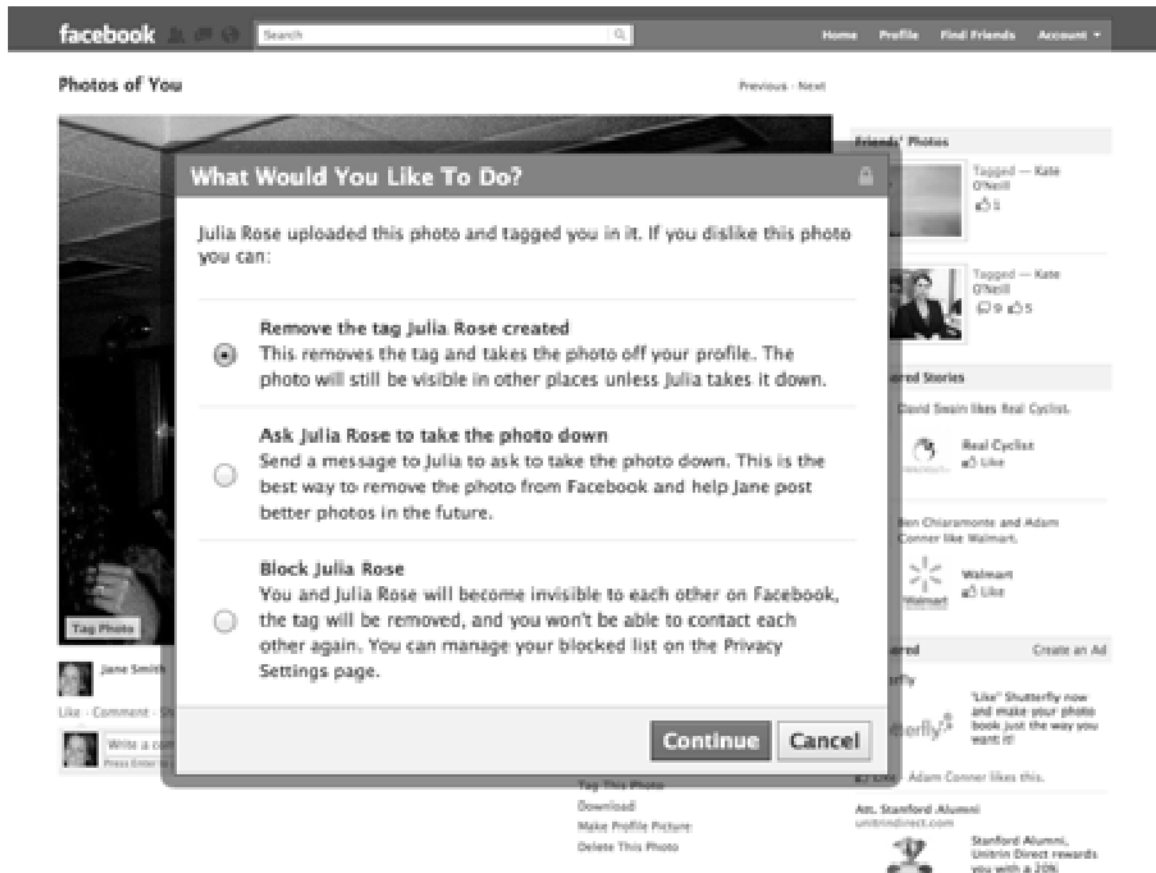
As a part of this, we are phasing out the mobile-only Places feature. Settings

associated with it are also being phased out or removed. (You can read more about how location works and settings affected here: <http://www.facebook.com/about/location>)

Remove tags or content from Facebook

Before: when we asked, people had different ideas of what removing a tag actually did, and different motivations for wanting to remove them.

Going forward: your options for removing tags or content on Facebook are presented more clearly. Your options are: removing from your profile, removing the tag itself, messaging the photo owner or tagger, and requesting the content get taken down. (More details on tagging can be found here: <http://www.facebook.com/about/tagging>).



These changes will start to roll out in the coming days. When they reach you, you'll see a prompt for a tour that walks you through these new features from your homepage. In the meantime, you can read more about the upcoming changes from the links throughout this post. We'll look forward to your feedback

on all of this.

Taken together, we hope these new tools make it easier to share with exactly who you want, and that the resulting experience is a lot clearer and a lot more fun.

From: Stephanie Kretschmer
Sent: 21 Jun 2011 19:50:31 +0000
To: JDL
Cc: Young, June
Subject: RE: Time to Talk

Hi Jon,

We are all set for 4pm PST/7pm EST today. I forwarded your note, by wanted to pass along Elliot's current email address:

(b)(6)

Thanks!

Stephanie M. Kretschmer
Executive Assistant to Elliot Schrage | Facebook
VP Global Communications, Marketing & Public Policy

(b)(6)

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

From: JDL [mailto:JDL@ftc.gov]
Sent: Monday, June 20, 2011 6:54 PM
To: (b)(6)
Cc: Young, June; Stephanie Kretschmer
Subject: Time to Talk

Hi Elliot,

I am running errands in the morning but should be in the office by 10:30 my time and free until about 11:15. Then I'm out of pocket until 2:00 but available most times after that.

Office direct line is 202.326.2533 and my cell is (b)(6)

(b)(6)

(b)(6)

Best,

Jon

Sent from JDL Blackberry