Independent Assessor's Report on Facebook's Privacy Program

Initial Assessment Report

For the period August 15, 2012 to February 11, 2013

pwc

Table of Contents

pwc

Introduction

Facebook, Inc. and the Federal Trade Commission (FTC) entered into Agreement Containing Consent Order File No: 0923184 ("the Order"), which was served on August 15, 2012.

Part IV of the Order requires Facebook to establish and implement, and thereafter maintain, a comprehensive privacy program that is reasonably designed to (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information.

Part V of the Order requires Facebook to obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. Facebook engaged PricewaterhouseCoopers LLP ("PwC") to perform the initial assessment.

As described on pages 6-13, Facebook established its privacy program by implementing privacy controls to meet or exceed the protections required by Part IV of the Order. As described on pages 14-17, PwC performed inquiry, observation, and inspection/examination procedures to assess the effectiveness of the Facebook privacy controls implemented to meet or exceed the protections required by Part IV of the Order during the first 180 day period ended February 11, 2013, and our conclusions are on pages 4-5.

pwc

Report of Independent Accountants

To the Management of Facebook, Inc.:

We have examined Management's Assertion, that as of and for the 180 days ended February 11, 2013 (the "Reporting Period"), in accordance with Parts IV and V of the Agreement Containing Consent Order (the "Order") with an effective date of service of August 15, 2012, between Facebook, Inc. ("Facebook" or "the Company") and the United States of America, acting upon notification and authorization by the Federal Trade Commission ("FTC"), the Company had established and implemented a comprehensive Privacy Program, as described in Management's Assertion ("the Facebook Privacy Program"), based on Company-specific criteria, and the privacy controls were 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.

The Company's management is responsible for the assertion. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and accordingly, included examining, on a test basis, evidence supporting the effectiveness of the Facebook Privacy Program as described above and performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

We are not responsible for Facebook's interpretation of, or compliance with, information security or privacy-related laws, statutes, and regulations applicable to Facebook in the jurisdictions within which Facebook operates. We are also not responsible for Facebook's interpretation of, or compliance with, information security or privacy-related self-regulatory frameworks. Therefore, our examination did not extend to the evaluation of Facebook's interpretation of or compliance with information security or privacy-related laws, statutes, regulations, and privacy-related self-regulatory frameworks with which Facebook has committed to comply.

In our opinion, Facebook's privacy controls were 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, in all material respects as of and for the 180 days ended February 11, 2013, based upon the Facebook Privacy Program set forth in Management's Assertion.

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

pwc

This report is intended solely for the information and use of the management of Facebook and the United States Federal Trade Commission and is not intended to be and should not be used by anyone other than these specified parties.

PricewaterhouseCoopers L.L.P.

San Jose

April 16, 2013

Facebook's Privacy Program Overview

Company Overview

Founded in 2004, Facebook's mission is to give people the power to share and make the world more open and connected. Facebook has been working on privacy since its inception and consistently strives to enhance various elements of its internal privacy programs. For example, Facebook now has a Privacy Cross-Functional ("XFN") internal team (comprised of experts with a range of privacy expertise) that vets and reviews products during the development cycle and before launch. Facebook also created two new corporate officer roles— Chief Privacy Officer, Product and Chief Privacy Officer, Policy—who are charged with ensuring that Facebook's commitments are reflected in all of its activities.

Facebook supports its mission by developing useful and engaging tools that enable people to connect, share, discover, and communicate with each other on mobile devices and computers. Facebook's products include News Feed, Timeline, Platform, Graph Search, Messages, Photos and Video, Groups, Events, and Pages. These products are available through Facebook's website, Facebook.com. They are also accessible through certain Facebook mobile applications or "apps", including Facebook, Camera, Messenger, Pages, and Poke. Versions of Facebook's mobile apps are available for multiple operating systems, such as iOS and Android operating systems. These products and services allow people all over the world to share, and communicate with each other in new and innovate ways, connecting people in ways not possible before these tools were offered.

Facebook Platform ("Platform") is a set of development tools and application programming interfaces ("APIs") that enable developers to build their own social apps, websites, and devices that integrate with Facebook. The Facebook's Developer Operations team is focused on supporting successful applications, driving platform adoption, and maintaining the user experience through developer education and policy enforcement. The Platform Principles that Facebook imposes on all developers are: (1) Create a great user experience (Build social and engaging applications; Give users choice and control; and Help users share expressive and relevant content); and (2) Be trustworthy (Respect privacy; Don't mislead, confuse, defraud, or surprise users; and Don't spam - encourage authentic communications). Additionally, Facebook's Statement of Rights and Responsibilities and Platform Policies outline a variety of developer obligations, including those around privacy, such as providing notice and obtaining consent for certain data uses and restrictions on sharing user information.

Most products and services Facebook offers are free. Facebook is able to do this by providing value for marketers, including brand marketers, small and medium-sized businesses, and developers. Facebook offers a unique combination of reach, relevance, social context, and engagement. Marketers can also use Facebook's analytics platform, Facebook Ad Analytics, to understand and optimize the performance of their campaigns.

In addition to Facebook created products and services, Facebook acquired Instagram on August 31, 2012. Instagram is a photo sharing service that enables users to take photos, apply digital filters to the photos, share them with others, and comment on photos posted by themselves or by others. At the time of acquisition, Instagram had approximately 13 employees. During the reporting period subsequent to the acquisition, Instagram was

available on the web at Instagram.com and as an app on the iOS and Android operating systems.

Facebook Privacy Program Scope

Facebook designed the 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 privacy and confidentiality of the information Facebook receives from or about consumers. Facebook leveraged the Generally Accepted Privacy Principles ("GAPP") framework, set forth by the American Institute of Certified Public Accountants ("AICPA") and Canadian Institute of Chartered Accountants ("CICA"), to define company-specific criteria for the foundation of the Facebook Privacy Program. The GAPP framework is globally recognized as a leading and comprehensive standard for privacy programs.

The ten GAPP principles, which are derived from internationally recognized information practices, are as follows:

1. **Management.** The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.

2. **Notice.** The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.

3. **Choice and consent.** The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.

4. **Collection.** The entity collects personal information only for the purposes identified in the notice.

5. **Use, retention, and disposal.** The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.

6. **Access.** The entity provides individuals with access to their personal information for review and update.

7. **Disclosure to third parties.** The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.

8. **Security for privacy.** The entity protects personal information against unauthorized access (both physical and logical).

9. **Quality.** The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.

10. **Monitoring and enforcement.** The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy related complaints and disputes.

The following is a brief description of the Facebook Privacy Program.

Facebook has designated a team of employees who are directly responsible for the Facebook Privacy Program (the "Privacy Governance Team"). Facebook's Chief Privacy Officer, Product leads the Privacy Governance Team. Other team members include the Chief Privacy Officer, Policy; Chief Security Officer, Associate General Counsel, Privacy; Associate General Counsel, Privacy and Product; Associate General Counsel, Advertising and Product; and Associate General Counsel, Regulatory. While the Chief Privacy Officer, Product provides leadership responsibility for coordinating the Privacy Program, the entire Privacy Governance Team and many employees (including engineers, product managers, etc.) are responsible for various aspects of the Privacy Program and play a crucial role driving and implementing decisions made by the Privacy Governance Team. Of particular note are the Privacy Program Managers who work directly under Chief Privacy Officer, Product. This team is embedded in the product organization and is responsible for: (1) engaging closely with legal, policy, and other members of the Privacy XFN Team to drive privacy decisions; (2) coordinating and presenting privacy issues to the Privacy XFN Team; and (3) maintaining records of privacy decisions and reviews.

A central aspect of Facebook's Privacy Program is a continuous assessment of privacy risks. As part of this risk assessment process, members of the Privacy Governance Team work with relevant Facebook stakeholders, including representatives of Facebook's Privacy, Engineering, Security, Internal Audit, Marketing, Legal, Public Policy, Communications, Finance, Platform Operations, and User Operations teams, to identify reasonably foreseeable, material risks, both internal and external, that could result in the unauthorized collection, use or disclosure of covered information. This process is enriched by input from the Chief Privacy Officer, Policy and her team, which engage with industry stakeholders and regulators and integrate external feedback into Facebook's program.

The team considers risks in each relevant area of operation, including governance, product design, and engineering (including product development and research), user operations (including third-party developers), advertising, service providers, employee awareness and training, employee management, and security for privacy. The team also considers the sufficiency of the safeguards in place to control the identified risks. Through this process, Facebook has documented reasonably foreseeable material risks to user privacy and has put in place reasonable privacy processes and controls to address those risks.

As part of Facebook's on-going privacy risk assessment process, Facebook holds an annual "Privacy Summit" of relevant stakeholders, including key representatives from the Privacy XFN Team. The Privacy XFN Team includes representatives from each major segment of Facebook, including Facebook's Privacy, Public Policy, Legal, Marketing, Product, Engineering, Security, and Communications teams. Attendees of the annual Privacy Summit review and update the privacy risk assessment, focusing on significant material risks identified by the Privacy Governance Team. Attendees evaluate those privacy risks in light of changing internal and external threats, changes in operations, and changes in laws and regulations. Attendees also examine the sufficiency of existing privacy controls in mitigating those risks, as well as new potential risks. Finally, attendees engage in discussion around ways to improve the work performed by the Privacy XFN Team. The last Privacy Summit occurred on January 15, 2013.

As indicated above, Facebook's Privacy Governance Team, led by the Chief Privacy Officer, Product is responsible for the design, implementation, and maintenance of the Privacy Program, which is documented in written policies and procedures. Highlights of the program are detailed below.

Privacy and Security Awareness Activities

Facebook communicates Privacy and Security awareness matters to new and existing employees and tailors such communications according to role and responsibility. For example, as part of its regular training for new project managers, Facebook trains project managers about the privacy program and key privacy considerations during the product development cycle. This training involves representatives from the Privacy XFN Team presenting to the project managers (the Privacy XFN process covers those directly involved in the development and management of new products, enhancements to existing products and services for consumers, as described below under "Product Design, Development and Research Activities). As a further example, engineers at Facebook spend their first six weeks in bootcamp, an immersive, cross-functional orientation program. During bootcamp, engineers are instructed on the importance of privacy and security at Facebook, along with their obligations to protect user information as it relates to their roles and responsibilities. Similar group-specific trainings are held for other constituents in the Company (e.g., user operations).

Facebook also holds "Hacktober" annually in October. Hacktober is a month-long event intended to increase employee privacy and security awareness. A series of simulated security threats (e.g., phishing scams) are presented to employees to determine how the employees would respond. If employees report the security threat, they receive a reward, such as Facebook-branded merchandise. If the security threat goes unreported, or if vulnerability is exploited, the employees undergo further education and awareness.

To further promote recognition and understanding of privacy issues and obligations among all Facebook employees, Facebook recently deployed, in addition to initiatives described above, a computer-based privacy training program to all employees. This training provides an overview of applicable privacy laws and Facebook's privacy commitments. All new employees are now required to complete the privacy training within 30 days of employment, while all existing employees are required to complete the privacy training annually. Facebook employees are quizzed on their understanding of Facebook's privacy practices during the training.

Product Design, Development, and Research Activities

The Privacy XFN Team considers privacy from the earliest stages in the product development process (i.e., "privacy by design"). The Chief Privacy Officer, Product and his team spearhead this review and lead a number of key functions and responsibilities. First, as described above, employees, including engineers, product managers, content strategists, and product marketing managers, are educated on Facebook's privacy framework. This education includes an overview of Facebook's processes and corresponding legal obligations, and may involve other members of the Privacy XFN team, such as Privacy and Product Counsel.

Second, the Chief Privacy Officer, Product and his team host weekly reviews of key product-related decisions and material changes to Facebook's privacy framework, which are attended by members of the Privacy XFN Team. The Chief Privacy Officer, Product and his team also review all new product proposals and any material changes to existing products from a privacy perspective and involve the Privacy XFN Team for broader review and feedback. The impact of privacy principles such as notice, choice, consent, access, security,

retention, deletion, and disclosure are considered as part of this review. Product launches are added to the Privacy Launch Calendar to ensure on-going review and consideration of privacy issues by the Privacy XFN Team throughout the development process. Members of the Privacy XFN Team also communicate back to their respective teams on issues covered in the weekly reviews. This review process helps ensure that privacy is considered throughout the product development process, and maintains consistency on privacy issues across all Facebook products and services.

The following products, available on the platforms and devices indicated, are included in the scope of Facebook's Privacy Program and the Order:

- Facebook: Facebook.com (internet/web), m.facebook.com, iOS, Android, Facebook for Every Phone, Facebook for Blackberry, Facebook for Windows;
- Messenger: iOS, Android;
- Camera: iOS;
- Pages Manager: iOS, Android;
- Poke: iOS; and
- Instagram: Instagram.com (internet/web), iOS, Android.

Facebook Platform

Platform applications and developers are required to comply with, and are subject to, Facebook's Statement of Rights and Responsibilities, Platform Principles, and Platform Policies. These terms and policies outline a variety of privacy obligations and restrictions, such as limits on an application's use of data received through Facebook, requirements that an application obtain consent for certain data uses, and restrictions on sharing user data. Facebook's Platform privacy setting and Granular Data Permissions ("GDP") process allows users to authorize the transfer of Facebook user information to third-party applications. Monitoring controls are in place to detect material misuse of the Platform (e.g., user complaints, third-party applications that do not have active privacy policy links).

Security for Privacy

Facebook has implemented technical, physical, and administrative security controls designed to protect user data from unauthorized access, as well as to prevent, detect, and respond to security threats and vulnerabilities. Facebook's security program is led by the Chief Security Officer ("CSO") and supported by a dedicated Security Team. As mentioned above, the CSO is a key and active member of the Privacy Governance team. Facebook's security and privacy employees work closely on an on-going basis to protect user data and Facebook's systems.

Monitoring Activities

In order to ensure that the effectiveness of its controls and procedures are regularly monitored, Facebook has designated an "owner" for each of the controls included in the Privacy Program. Facebook utilizes the annual Privacy Summit to monitor the effectiveness of controls and procedures in light of changing internal and external risks. In addition, members of Facebook's Legal team periodically review the Privacy Program to ensure it, including the controls and procedures contained therein, remains effective. These Legal team members also will serve as point of contacts for control owners and will update the Privacy Program to reflect any changes or updates surfaced.

Service Providers

Facebook has implemented controls with respect to third-party service providers, including implementing policies to select and retain service providers capable of appropriately protecting the privacy of covered information received from Facebook.

Facebook's Security team has a process for conducting due diligence on service providers who may receive covered information in order to evaluate whether their data security standards are aligned with Facebook's commitments to protect covered information. As part of the due diligence process, Facebook asks prospective service providers to complete a security architecture questionnaire or vendor security questionnaire to assess whether the provider meets Facebook's functional security requirements to protect the privacy of user data. Based upon the service provider's responses to the vendor security questionnaire and other data points, Facebook's Security team determines whether further security auditing is required. Facebook partners with an outside security consulting firm to conduct security audits, which may include testing of the service provider's controls, a vulnerability scanning program, a web application penetration test, and/or a code review for security defects. The security consulting firm reports its findings to Facebook, and Facebook requires that the prospective service provider fix critical issues before being on-boarded. Depending on the sensitivity of Facebook data shared with the service provider and other factors, Facebook may require that the service provider undergo a periodic or random security and/or privacy audit.

Facebook also has a contract policy (the "Contract Policy"), which governs the review, approval, and execution of contracts for Facebook. Facebook's pre-approved contract templates require service providers to implement and maintain appropriate protections for covered information. Facebook reviews contracts that deviate from the pre-approved templates to help ensure that contracts with applicable service providers contain the required privacy protections. Facebook Legal documents review of any such contracts through formal approval prior to contract execution.

Monitoring

Facebook's Privacy Program is designed with procedures for evaluating and adjusting the Privacy Program in light of the results of testing and monitoring of the program as well as other relevant circumstances. As mentioned above, Facebook's annual Privacy Summit is designed to identify, discuss, and assess compliance with privacy policies and procedures, and applicable laws and regulations, as well as identify new or changed risks and recommend responsive controls. The Privacy XFN Team assesses risks and controls on an on-going basis through weekly meetings and review processes. Members of Facebook's Legal team support the Privacy Program and serve as points of contact for all relevant control owners to communicate recommended adjustments to the Privacy Program based on regular monitoring of the controls for which they are responsible, as well as any internal or external changes that affect those controls. Additionally, the Privacy Governance Team regularly discusses the Privacy Program in the context of various product and operational discussions. During these discussions, the effectiveness and efficiency of the Privacy Program are considered and reviewed and, when appropriate, adjustments are made to maintain a strong program.

Facebook also continuously evaluates acquisitions for inclusion in the Privacy Program, based on the nature of the acquisition (e.g., talent or people, intellectual property, product or infrastructure). Specifically, Facebook takes steps, as appropriate, to integrate acquisitions into the Privacy Program and reviews products and features developed by acquisitions with the same level of rigor applied to Facebook's products and services. The acquisitions in the current Reporting Period were primarily talent acquisitions, except for Instagram. Instagram's people, product, and supporting infrastructure were acquired on August 31, 2012.

Facebook assessed the privacy risks associated with Instagram's people, process, and technology upon acquisition. In comparison to Facebook, Instagram has significantly fewer users, employees, and products. As described in the Company Overview above, Instagram's products focus on photo taking, filtering, and sharing. From a privacy perspective, Instagram users have one binary choice - to make all photos private or all photos public by setting the "Photos are Private" on/off slider. Once private, the user approves any "follower" requests. After obtaining approval, the follower can access posted photos and related comments. The Privacy XFN Team also was involved in reviewing Instagram's January 19, 2013 privacy policy update.

PwC's Privacy Assessment Approach

PwC's Assessment Standards

Part V of the Order requires that the Assessments be performed by a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. This report was issued by PwC under professional standards which meet these requirements.

As a public accounting firm, PwC must comply with the public accounting profession's technical and ethical standards, which are enforced through various mechanisms created by the American Institute of Certified Public Accountants ("AICPA"). Membership in the AICPA requires adherence to the Institute's Code of Professional Conduct. The AICPA's Code of Professional Conduct and its enforcement are designed to ensure that CPAs who are members of the AICPA accept and achieve a high level of responsibility to the public, clients, and colleagues. The AICPA Professional Standards provide the discipline and rigor required to ensure engagements performed by CPAs consistently follow specific General Standards, Standards of Fieldwork, and Standards of Reporting ("Standards").

In order to accept and perform this FTC assessment ("engagement"), the Standards state that PwC, as a practitioner, must meet specific requirements, such as the following.

General Standards:

- Have reason to believe that the subject matter is capable of evaluation against criteria that are suitable and available to users. Suitable criteria must be free from bias (objective), permit reasonably consistent measurements, qualitative or quantitative, of subject matter (measurable), be sufficiently complete so that those relevant factors that would alter a conclusion about subject matter are not omitted (complete), and be relevant to the subject matter;
- Have adequate technical training and proficiency to perform the engagement;
- Have adequate knowledge of the subject matter; and
- Exercise due professional care in planning and performance of the engagement and the preparation of the report.

Standards of Fieldwork:

- Adequately plan the work and properly supervise any assistants; and
- Obtain sufficient evidence to provide a reasonable basis for the conclusion that is expressed in the report.

Standards of Reporting:

- Identify the assertion being reported on in the report; and
- State the practitioner's conclusion about the assertion in relation to the criteria.

In performing this assessment, PwC complied with all of these Standards.

pwc

Independence

The Standards also require us to maintain independence in the performance of professional services. Independence requirements fall into five categories: personal financial interests; business relationships; employment relationships; prohibited services; prohibition from serving in the Company's management capacity; and independence in mental attitude. In summary, relevant individuals must not have personal financial interests in the Company; the Company and the Assessor may not have certain business relationships; there are restrictions on relationships that may exist between employees performing the assessment and employees at the Company or formerly at the Company or at the Assessor firm; there are numerous services that cannot be provided by the Assessor to the Company; and the Assessor may not act in a management capacity or make any decisions for the Company.

Further, the Standards require us to maintain independence in mental attitude in all matters relating to the engagement. Independence in mental attitude means there is an objective consideration of facts, unbiased judgments, and honest neutrality on the part of the practitioner in forming and expressing conclusions. We are required to maintain intellectual honesty and impartiality necessary to reach an objective and unbiased conclusion.

PwC is independent with respect to the Standards required for this engagement.

PwC Assessor Qualifications

PwC assembled an experienced, cross-disciplinary team of PwC team members with privacy, assessment, and technology industry expertise to perform the Assessor role for the Order. A Partner in PwC's Data Protection and Privacy practice with more than 32 years of experience providing professional services led the engagement. The assessment was performed by an experienced team of over thirteen professionals with a combination of privacy, data protection, information security, industry, and assessment experience. The team included Certified Information Privacy Professionals ("CIPP"), Certified Information Systems Auditors ("CISA"), and Certified Public Accountants ("CPA"). To ensure quality, a Quality Assurance Partner was involved as well as Risk Management personnel from PwC's National Professional Services team.

PwC's procedures lasted over fifteen weeks. The fieldwork was primarily performed at Facebook's headquarters in Menlo Park, CA, with the exception of data center physical and environment control testing. Instagram is also located at Facebook's headquarters.

PwC Assessment Process Overview

The procedures performed by PwC were designed to:

- Assess the applicability of management's assertion to address the Company's obligations within Part IV of the Order;
- Assess the design effectiveness of the control activities implemented by the Company to address the relevant sections of the management assertion; and
- Assess the operating effectiveness of the implemented control activities for the 180-day period ended February 11, 2013.

pwc

PwC designed and performed test procedures to evaluate the design effectiveness and operating effectiveness of the control activities implemented by Facebook for the 180 days ended February 11, 2013. For the Instagram-only controls, PwC tested controls from the date of acquisition of Instagram, August 31, 2012 through to February 11, 2013. Where Instagram processes and controls were maintained separately during the period, PwC tested the Instagram-only controls separately. Where Instagram processes and controls were integrated into the Facebook privacy program, PwC included Instagram as part of our testing of Facebook's processes and controls.

The nature of PwC's testing was dependent on each control, and PwC developed a test plan based on our understanding of the risk, complexity, extent of judgment and other factors. We used a combination of inquiry, observation and/or inspection for testing of the controls. Refer below for a description of the test procedures utilized by PwC:

> Inquiry: To understand the design of the controls implemented and how they operate to meet or exceed the protections required by Part IV of the order, PwC had discussions with Facebook personnel. The inquiry procedures included asking the Facebook personnel about relevant controls, policies and procedures, as well as roles and responsibilities. To validate the information obtained in the discussions, PwC performed corroborative inquiry procedures with multiple individuals and, using the testing techniques below, obtained additional evidence to validate the responses.
>
> Observation: PwC utilized the observation testing method to validate the design and operating effectiveness of controls. In areas where Facebook has implemented controls that meet or exceed the protections required by Part IV of the order, the PwC team met with relevant Facebook personnel and observed how the control is designed and how it functions. For example, PwC attended Privacy XFN meetings to observe first-hand the operation of this control. PwC watched the attendees interact, discuss products and policy changes, and assess the potential impact on the users and the Privacy Program.
>
> Examination or inspection of evidence: PwC used the examination and/or inspection test approach to validate the operating effectiveness of controls and to evaluate the sufficiency of controls implemented to address Part IV of the Order. PwC inspected, physically or online, artefacts and documents (including documentation of the company's policies and procedures, risk assessment, training, and awareness programs) to evidence the design and operating effectiveness of the controls and safeguards implemented. The nature of the evidence examined varied from control to control and, where appropriate, other procedures like observation and inquiry were utilized to confirm the results of the examination procedures.

To assess design effectiveness, PwC performed walkthroughs of the processes and controls to determine whether the controls were built to achieve the intended assertions as well as to determine whether the controls had been placed into operation. To perform a walkthrough, PwC met with relevant Facebook control owners. Additionally, during the design assessment, PwC assessed whether the persons performing the controls possessed the necessary authority and competence to perform the controls effectively. Our design effectiveness test procedures included performing a combination of inquiry, observation, and/or inspection/ examination.

To assess operating effectiveness, PwC performed procedures to determine whether controls were executed by Facebook (or Facebook's systems if automated) on a regular frequency and whether documentation and/or support was maintained to evidence the controls' execution. Our operating effectiveness test procedures included, where appropriate, selecting samples from throughout the period and performing a combination of inquiry, observation, and/or inspection/ examination procedures to evaluate the effectiveness of the Facebook control activities documented on pages 21-76 of this document.

Over the course of the reporting period, PwC performed procedures that included interviewing individuals from Privacy, Legal, Identity, Security, User Operations, Developer Operations, Engineering, Infrastructure, Mobile Partner Management, and Human Resources. Test plans for each control activity tested are also included on pages 21-76 of this document. See Appendix A for a summary of interviewees.

pwc

PwC's Assessment of Part IV A, B, C, D and E, of the Order

The tables in section "Facebook's Privacy Program: Assertions, Control Activities and PwC's Tests Performed and Results" of this report describe the scope of Facebook's Privacy Program referenced in the Management Assertion on pages 77-78. Facebook established its privacy program by implementing privacy controls to meet or exceed the protections required by Part IV of the Order. The table also includes PwC's inquiry, observation, and inspection/examination test procedures to assess the effectiveness of Facebook's program and test results. PwC's final conclusions are detailed on pages 4-5 of this document.

A. Set forth the specific privacy controls that respondent has implemented and maintained during the reporting period.

As depicted within the table on pages 21-76, Facebook has listed the privacy controls that were implemented and maintained during the reporting period.

B. Explain how such privacy controls are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the covered information.

Based on the size and complexity of the organization, the nature and scope of Facebook's activities, and the sensitivity of the covered information (as defined in by the order), Facebook management developed the company-specific criteria (assertions) detailed on pages 77-78 as the basis for its Privacy Program. The management assertions and the related control activities are intended to be implemented to address the risks identified by Facebook's privacy risk assessment.

C. Explain how the privacy controls that have been implemented meet or exceed the protections required by Part IV of the Order.

As summarized in the Facebook's Privacy Program on pages 6-13, Facebook has implemented the following protections:

> A. Designation of an employee or employees to coordinate and be responsible for the privacy program.
>
> As described above, Facebook has designated a team of employees to coordinate and be responsible for the Privacy Program as required by Part IV of the Order. As described on pages 21-23 (Management's Assertion A), PwC performed test procedures to assess the effectiveness of the Facebook privacy controls implemented to meet or exceed the protections required by Part IV of the Order.
>
> B. The identification of reasonably foreseeable, material risks, both internal and external, that could result in Respondent's unauthorized collection, use, or disclosure of covered information and an assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this privacy risk assessment should include consideration of risks in each area of relevant operation,

including, but not limited to: (1) employee training and management, including training on the requirements of this order, and (2) product design, development, and research.

As described above, Facebook has identified reasonably foreseeable, material risks, both internal and external, that could result in Facebook's unauthorized collection, use, or disclosure of covered information, and assessed the sufficiency of any safeguards in place to control these risks as required by Part IV of the Order. As described on page 24 (Management's Assertion B), PwC performed test procedures to assess the effectiveness of the Facebook privacy controls implemented to meet or exceed the protections required by Part IV of the Order.

C. The design and implementation of reasonable controls and procedures to address the risks identified through the privacy risk assessment, and regular testing or monitoring of the effectiveness of those controls and procedures.

As described above, Facebook has designed and implemented 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 as required by Part IV of the Order. As described on pages 25-65 (Management's Assertions C, D, E, F, and G), PwC performed test procedures to assess the effectiveness of the Facebook privacy controls implemented to meet or exceed the protections required by Part IV of the Order.

D. The development and use of reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from Respondent and requiring service providers, by contract, to implement and maintain appropriate privacy protections for such covered information.

As described above, Facebook has developed and implemented reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from Facebook as required by Part IV of the Order. Facebook also includes terms in contracts with service providers requiring that such service providers implement and maintain appropriate privacy protections. As described on pages 66-70 (Management's Assertion H), PwC performed test procedures to assess the effectiveness of the Facebook privacy controls implemented to meet or exceed the protections required by Part IV of the Order.

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

As described above, Facebook has evaluated and adjusted its Privacy Program in light of the results of the testing and monitoring required by subpart C within Part IV of the Order, any material changes to Facebook's operations or business arrangements, or any other circumstances that Facebook knows or has reason to

know may have a material impact on the effectiveness of its privacy program as required by Part IV of the Order. As described on pages 71-76 (Management's Assertion I), PwC performed test procedures to assess the effectiveness of the Facebook privacy controls implemented to meet or exceed the protections required by Paragraph IV of the Order.

D. Certify that the privacy controls are operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the reporting period.

As described in the PwC Assessment Process Overview section above, PwC performed its assessment of Facebook's Privacy Program in accordance with AICPA Attestation Standards. Refer to pages 4-5 of this document for PwC's conclusions.

Facebook's Privacy Program: Assertions, Control Activities and PwC's Tests Performed and Results

Provided below are the Facebook Privacy Program controls and PwC's tests performed. Also provided are the results of the testing performed by PwC. Finally, additional information has been provided by PwC for the instances in which PwC identified an exception during testing. This information is provided in an effort to enhance the FTC's understanding of the exception. Unless otherwise indicated in the table below, exceptions identified relate to the Reporting Period (August 15, 2012 to February 11, 2013) for Facebook or from the date of acquisition to the end of the Reporting Period (August 31, 2012 to February 11, 2013) for Instagram.

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion A – Responsibility for the Facebook Privacy Program Facebook has designated an employee or employees to coordinate and be responsible for the privacy program.				
A-1	Facebook has designated a team of employees who are directly responsible for the Privacy Program (the "Privacy Governance Team"). Facebook's Chief Privacy Officer, Product leads the Privacy Governance Team.	(b)(3):6(f),(b)(4)		
A-2	Facebook has designated a team of employees who are directly responsible for the Information Security Program (the "Security Team"). Facebook's Chief Security Officer leads the Security Team.			
A-3	Facebook has defined roles and responsibilities for teams supporting the Privacy and Information Security Programs, including: • Privacy Governance Team - Responsible for coordinating Facebook's Privacy Program, which is led by the Chief Privacy Officer, Product. The Privacy			

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion A – Responsibility for the Facebook Privacy Program				
Facebook has designated an employee or employees to coordinate and be responsible for the privacy program.				
	Governance Team is integrated into the product development process and leads Facebook's commitment to build privacy into its products at an early stage of development. • Privacy Cross Functional Team (XFN) - Includes representatives from major segments of Facebook, including: Privacy Governance team, Policy, Legal, Marketing, Product, Engineering, Security, and Communications. Responsible for the product development process and leads Facebook's commitment to build privacy into its products at an early stage of development. • Information Security Team - Responsible for coordinating Facebook's Security Program, which is led by the Chief Security Officer. The Information Security Team is integrated as part of the Privacy XFN Team, and is responsible for ensuring that security for privacy programs, policies and procedures are implemented within the organization.	(b)(3):6(f),(b)(4)		
A-4	Facebook has defined and documented qualifications for key positions that are directly responsible for the privacy and security of user information.			

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion A – Responsibility for the Facebook Privacy Program				
Facebook has designated an employee or employees to coordinate and be responsible for the privacy program.				
A-5	Facebook's hiring procedures establish the due diligence procedures (i.e., background checks) needed to ensure personnel responsible for protecting privacy and security are qualified.	(b)(3):6(f),(b)(4)		

pwc

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion B – Privacy Risk Assessment Facebook has identified reasonably foreseeable, material risks, both internal and external, that could result in Facebook's unauthorized collection, use, or disclosure of covered information and an assessment of the sufficiency of any safeguards in place to control these risks. This privacy risk assessment includes consideration of risks in areas of relevant operations, including, but not limited to: (1) employee training and management, including training on the requirements of this order, and (2) product design, development, and research.				
B-1	Facebook holds an Annual Privacy Summit of relevant stakeholders, including key representatives from the Privacy Cross-Functional (XFN) Team. The attendees of the Annual Privacy Summit review and update the privacy risk assessment, focusing on significant material risks identified by the Privacy Governance Team. The attendees also evaluate those privacy risks in light of changing internal and external threats, changes in operations, and changes in laws and regulations. The sufficiency of existing controls is considered in mitigating identified risks.	(b)(3):6(f),(b)(4)		

pwc

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion C. Privacy and Security (for Privacy) Awareness Facebook has a privacy and security for privacy awareness program in place which is defined and documented in privacy and security for privacy policies. The extent of communications to employees is based on their role and responsibility and may include internal communications through various channels, training, and the Privacy Cross-Functional ("XFN") team process.				
C-1	Facebook's privacy policy is called the "Data Use Policy." Facebook's terms of service are outlined in the "Statement of Rights and Responsibilities," which governs Facebook's relationship with users and others who interact with Facebook. Instagram maintains a separate privacy policy and terms of service. The topics covered within these policies include the following: • Notice • Choice and consent • Collection • Use, retention, and deletion • Access • Disclosure to third parties • Security for privacy • Quality • Monitoring and enforcement	(b)(3):6(f),(b)(4)		
C-2	(b)(3):6(f),(b)(4)			

pwc

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion C. Privacy and Security (for Privacy) Awareness Facebook has a privacy and security for privacy awareness program in place which is defined and documented in privacy and security for privacy policies. The extent of communications to employees is based on their role and responsibility and may include internal communications through various channels, training, and the Privacy Cross-Functional ("XFN") team process.				
	(b)(3):6(f),(b)(4)			
C-3	The information security policy and other supporting internal procedures are available to all employees via an internal site.	(b)(3):6(f),(b)(4)		
C-4	(b)(3):6(f),(b)(4)			

pwc

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion C. Privacy and Security (for Privacy) Awareness Facebook has a privacy and security for privacy awareness program in place which is defined and documented in privacy and security for privacy policies. The extent of communications to employees is based on their role and responsibility and may include internal communications through various channels, training, and the Privacy Cross-Functional ("XFN") team process.				
	(b)(3):6(f),(b)(4)			
C-5	Facebook and Instagram communicate their privacy policies and terms of service via the Facebook and Instagram external facing websites and across all available platforms and products. Material changes to Facebook's privacy policies and terms of service are communicated via company-wide notification channels, which includes the: • Internal site; • Company-wide privacy training programs; and • Facebook's Site Governance page, which is the site where proposed changes to the Data Use Policy and Statement of Rights and Responsibilities are made available to the Facebook community for seven (7) days. The Site Governance page is intended to facilitate open-forum discussion of proposed changes to the Data Use Policy and Statement of Rights and Responsibilities, before the changes are put into effect.	(b)(3):6(f),(b)(4)		
C-6	(b)(3):6(f),(b)(4)			

pwc

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion C. Privacy and Security (for Privacy) Awareness				
Facebook has a privacy and security for privacy awareness program in place which is defined and documented in privacy and security for privacy policies. The extent of communications to employees is based on their role and responsibility and may include internal communications through various channels, training, and the Privacy Cross-Functional ("XFN") team process.				
	(b)(3):6(f),(b)(4)			

pwc

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion C. Privacy and Security (for Privacy) Awareness Facebook has a privacy and security for privacy awareness program in place which is defined and documented in privacy and security for privacy policies. The extent of communications to employees is based on their role and responsibility and may include internal communications through various channels, training, and the Privacy Cross-Functional ("XFN") team process.				
				(b)(3):6(f),(b)(4)

pwc

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion C. Privacy and Security (for Privacy) Awareness Facebook has a privacy and security for privacy awareness program in place which is defined and documented in privacy and security for privacy policies. The extent of communications to employees is based on their role and responsibility and may include internal communications through various channels, training, and the Privacy Cross-Functional ("XFN") team process.				
				(b)(3):6(f),(b)(4)
C-7	(b)(3):6(f),(b)(4)			

pwc

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion C. Privacy and Security (for Privacy) Awareness Facebook has a privacy and security for privacy awareness program in place which is defined and documented in privacy and security for privacy policies. The extent of communications to employees is based on their role and responsibility and may include internal communications through various channels, training, and the Privacy Cross-Functional ("XFN") team process.				
				(b)(3):6(f),(b)(4)
C-8	The Security Team conducts month long company-wide security awareness activities during National Cyber Security Awareness Month (October). Facebook refers to these activities as "Hacktober." Hacktober activities are intended to increase the awareness and visibility of security responsibilities and issues amongst Facebook employees.	(b)(3):6(f),(b)(4)		
C-9	Facebook has a Privacy Cross-Functional (XFN) team that is responsible for reviewing product launches, major changes, and privacy-related bug fixes to products and features to ensure that privacy policies and procedures are consistently applied. The Privacy XFN team is represented by members from the following major segments of Facebook: Privacy & Public Policy; Legal; Marketing;			

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion C. Privacy and Security (for Privacy) Awareness Facebook has a privacy and security for privacy awareness program in place which is defined and documented in privacy and security for privacy policies. The extent of communications to employees is based on their role and responsibility and may include internal communications through various channels, training, and the Privacy Cross-Functional ("XFN") team process.				
	Product; Engineering; Security; and Communications. Product launches, major changes and privacy-related bug fixes are added to the launch calendar for review and consideration of privacy by the XFN team. The XFN team meets on a weekly basis to review each new or modified product and/or feature launch to ensure that privacy policies and procedures are consistently applied. The XFN process ensures that new products and changes to existing products that result in material and/or retroactive changes to the use of information are evaluated to determine whether additional notice or consent from Facebook users is required. Where required, key decisions around the need for additional consent from users are discussed and recommendations are made and implemented by the XFN team.	(b)(3):6(f),(b)(4)		
C-10	Instagram only: New Instagram products/features and changes to existing products/features were not incorporated into Facebook's XFN process (Control C-9) until November 2012. Prior to this time, Instagram had a separate process, which included: • Developing a detailed product plan including project goals and a problem statement; and • Performing detailed testing of the			

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion C. Privacy and Security (for Privacy) Awareness Facebook has a privacy and security for privacy awareness program in place which is defined and documented in privacy and security for privacy policies. The extent of communications to employees is based on their role and responsibility and may include internal communications through various channels, training, and the Privacy Cross-Functional ("XFN") team process.				
	functionality of the new product, as well as the product's impact on privacy prior to launch.			

pwc

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion D. Notice, Choice, Consent, Collection and Access				
Facebook provides notice about its privacy policies and procedures and terms of service to users which identifies the purposes for which personal information is collected and used, describes the choices available to users, obtains implicit or explicit consent, collects personal information only for the purposes identified in the notices and provides users with access to their personal information for review and update.				
D-1	The privacy policies for Facebook and Instagram are: • In plain and simple language. • Appropriately labeled, easy to see, and not in unusually small print. • Available in many languages used on the site. • Describes the companies' operations and the types of information covered. • Readily accessible and available when personal information is first collected from the individual. • Provided in a timely manner (that is, at or before the time personal information is collected, or as soon as practical thereafter) to enable individuals to decide whether or not to submit personal information. • Clearly dated to allow individuals to determine whether the privacy practices have changed since the last time they read it or since the last time they submitted personal information.	(b)(3):6(f),(b)(4)		
D-2	Notice of proposed changes is provided to the privacy policy to all current users.			

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion D. Notice, Choice, Consent, Collection and Access				
Facebook provides notice about its privacy policies and procedures and terms of service to users which identifies the purposes for which personal information is collected and used, describes the choices available to users, obtains implicit or explicit consent, collects personal information only for the purposes identified in the notices and provides users with access to their personal information for review and update.				
		(b)(3):6(f),(b)(4)		
D-3	(b)(3):6(f),(b)(4)			

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion D. Notice, Choice, Consent, Collection and Access Facebook provides notice about its privacy policies and procedures and terms of service to users which identifies the purposes for which personal information is collected and used, describes the choices available to users, obtains implicit or explicit consent, collects personal information only for the purposes identified in the notices and provides users with access to their personal information for review and update.				
				(b)(3):6(f),(b)(4)
D-4	Facebook and Instagram obtain the user's explicit consent at the time of account creation.	(b)(3):6(f),(b)(4)		

pwc

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion D. Notice, Choice, Consent, Collection and Access Facebook provides notice about its privacy policies and procedures and terms of service to users which identifies the purposes for which personal information is collected and used, describes the choices available to users, obtains implicit or explicit consent, collects personal information only for the purposes identified in the notices and provides users with access to their personal information for review and update.				
	A user enters certain 'basic' personal information (e.g., first name, last name, email address, date of birth and gender information) and clicks on the "Sign Up" button. By clicking this button, the user chooses to share the information with Facebook, make this information public and be searchable online. If an individual chooses not to share any of this information, he or she cannot create a user account.	(b)(3):6(f),(b)(4)		
D-5	Facebook provides users with explicit and implicit notice of the in-line privacy settings			

pwc

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion D. Notice, Choice, Consent, Collection and Access Facebook provides notice about its privacy policies and procedures and terms of service to users which identifies the purposes for which personal information is collected and used, describes the choices available to users, obtains implicit or explicit consent, collects personal information only for the purposes identified in the notices and provides users with access to their personal information for review and update.				
	available within Facebook at the time of posting content (e.g., comment, photo, check-in, etc.).	(b)(3):6(f),(b)(4)		
D-6	Instagram only: By clicking on the "Register" button after entering required information (email address), the user chooses to share the information with Instagram and to make certain information public (e.g., pictures) and searchable online. The information requested during sign-up is required. If an individual chooses not to share any of this information, he or she cannot create a user account. The user is able can change privacy settings associated with posting photos, "follow" and "block" other Instagram user accounts from viewing posted photos and "like" photos from other Instagram users.			

pwc

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion D. Notice, Choice, Consent, Collection and Access Facebook provides notice about its privacy policies and procedures and terms of service to users which identifies the purposes for which personal information is collected and used, describes the choices available to users, obtains implicit or explicit consent, collects personal information only for the purposes identified in the notices and provides users with access to their personal information for review and update.				
		(b)(3):6(f),(b)(4)		
D-7	The Privacy XFN process ensures that new products and changes to existing products that result in material and/or retroactive changes to the use of information are evaluated to determine whether additional notice or consent is required. Where required, key decisions around the need for additional consent from users are discussed and recommendations are made by the XFN team.			

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion D. Notice, Choice, Consent, Collection and Access Facebook provides notice about its privacy policies and procedures and terms of service to users which identifies the purposes for which personal information is collected and used, describes the choices available to users, obtains implicit or explicit consent, collects personal information only for the purposes identified in the notices and provides users with access to their personal information for review and update.				
		(b)(3):6(f),(b)(4)		
D-8	Instagram only: New Instagram products/features and changes to existing products/features were not incorporated into Facebook's XFN process until November 2012. Prior to this time, Instagram had a separate process, which included: • Putting together a detailed product plan including project goals and a problem statement; and • Performing detailed testing of the functionality of the new product, as well as the product's impact on privacy.			
D-9	The Facebook and Instagram privacy policies disclose the use of cookies, pixels, and local storage and the types of uses for which those technologies are utilized. The user is advised that they may have device or browser options to block or remove cookies or other data stored on their computer or device and that doing so may limit their ability to use Facebook's products and services.			

pwc

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion D. Notice, Choice, Consent, Collection and Access Facebook provides notice about its privacy policies and procedures and terms of service to users which identifies the purposes for which personal information is collected and used, describes the choices available to users, obtains implicit or explicit consent, collects personal information only for the purposes identified in the notices and provides users with access to their personal information for review and update.				
	The privacy policy is made available to users at the time of account creation. By clicking on the "Sign Up" or "Register" button during account creation, the user provides consent for Facebook and Instagram to utilize these technologies.	(b)(3):6(f),(b)(4)		
D-10	Facebook's Data Use Policy and Instagram's privacy policy addresses the following: • Collection of user information. For example, the "Information we receive about you" section describes the different types of information collected from users. • Discloses to users the different types of information collected about them and the sources of the information collected. • The types of personal information collected from users and the general methods of collection. • How a user can access or download their information. • The company may develop and acquire information about the individual using third-party sources, browsing, credit and purchasing history.			

pwc

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion D. Notice, Choice, Consent, Collection and Access				
Facebook provides notice about its privacy policies and procedures and terms of service to users which identifies the purposes for which personal information is collected and used, describes the choices available to users, obtains implicit or explicit consent, collects personal information only for the purposes identified in the notices and provides users with access to their personal information for review and update.				
D-11	Facebook users and non-users can access their personal information via the following methods: (1) By logging into their active Facebook account to review, update, delete or correct information previously provided. (2) By downloading a copy of the information they have provided Facebook by visiting "Account Settings" and clicking on "Download a copy of your Facebook data" on facebook.com. This takes you to the "Download Your Information" (DYI) tool. Once the archive has been systematically generated, an email is sent to the email address on record for the user with a link to the file(s). The user is required to re-authenticate by entering his or her Facebook account password. (3) By downloading publicly available information through Facebook's Graph API by typing https://www.facebook.com/[User ID or Username]?metadata=1 into their browser. (4) By requesting access to their data by clicking the "Personal data requests" link under "Help" on Facebook.com. Facebook responds within a reasonable period of time, typically 40 days. UO tracks and documents responses to user data access requests using the TPS system. Facebook holds limited information for non-users (usually limited to e-mail address), which is stored on behalf of the user who shared that information.	(b)(3):6(f),(b)(4)		

pwc

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion D. Notice, Choice, Consent, Collection and Access Facebook provides notice about its privacy policies and procedures and terms of service to users which identifies the purposes for which personal information is collected and used, describes the choices available to users, obtains implicit or explicit consent, collects personal information only for the purposes identified in the notices and provides users with access to their personal information for review and update.				
D-12	Instagram only Instagram users can access their personal information via the following methods: (1) By logging into their Instagram account to review, update, delete or correct information previously provided. (2) By requesting any personal information associated with their account (e.g., pictures, email, and phone number) through the Help Center.	(b)(3):6(f),(b)(4)		
D-13	Facebook does not deny active users access to their personal information displayed on Facebook.com, unless the user violates Facebook's policies, and/or the users' account has been compromised or excessive login attempts have been made. In the event a user account is disabled for violating Facebook's policies, Facebook will communicate to the user, upon his or her attempt to log in, why access has been denied. Users may appeal the disablement via email to Facebook. These appeals are tracked via TPS tickets. In the event a user encounters a login issue and cannot access their account because the account has been compromised, Facebook offers ways for the user to regain access to his or her account through the Facebook Help Center.			

pwc

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion E - Use, Retention, Deletion and Quality Facebook limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. Facebook retains personal information for as long as necessary to provide services or fulfil the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information. Facebook maintains accurate, complete, and relevant personal information for the purposes identified in the notice.				
E-1	The privacy policy and terms of service addresses the use, retention, and deletion of user information, as well as the deletion and retention of individual content.	(b)(3):6(f),(b)(4)		
E-2	The Privacy XFN process ensures that uses of data are evaluated to determine whether additional notice or consent is required. Where required, key decisions around the need for additional consent from users are discussed and recommendations are made by the XFN team.			
E-3	(b)(3):6(f),(b)(4)			
E-4				

pwc

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion E - Use, Retention, Deletion and Quality				
Facebook limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. Facebook retains personal information for as long as necessary to provide services or fulfil the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information. Facebook maintains accurate, complete, and relevant personal information for the purposes identified in the notice.				
E-5	(b)(3):6(f),(b)(4)			
E-6				

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion E - Use, Retention, Deletion and Quality				
Facebook limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. Facebook retains personal information for as long as necessary to provide services or fulfil the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information. Facebook maintains accurate, complete, and relevant personal information for the purposes identified in the notice.				
E-7	(b)(3):6(f),(b)(4)	(b)(3):6(f),(b)(4)		
E-8	Instagram only: When a user requests their Instagram account to be deleted, the user's account, photos and comments are no longer viewable by other Instagram users.			
E-9	(b)(3):6(f),(b)(4)			

pwc

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion E - Use, Retention, Deletion and Quality Facebook limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. Facebook retains personal information for as long as necessary to provide services or fulfil the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information. Facebook maintains accurate, complete, and relevant personal information for the purposes identified in the notice.				
E-10	Facebook's Statement of Rights and Responsibilities contains a section stating that users consent to not provide any false personal information on Facebook and have the responsibility to keep such information accurate and up-to-date.	(b)(3):6(f),(b)(4)		

pwc

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion F - Security for Privacy				
Facebook protects personal information of users against unauthorized access.				
F-1	A program is established to maintain and increase the security awareness of employees.	(b)(3):6(f),(b)(4)		
F-2	(b)(3):6(f),(b)(4)			
F-3				

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion F - Security for Privacy				
Facebook protects personal information of users against unauthorized access.				
F-4	(b)(3):6(f),(b)(4)			
F-5				
F-6				
F-7				

pwc

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion F - Security for Privacy				
Facebook protects personal information of users against unauthorized access.				
F-8	Facebook's systems are configured to enforce strong passwords for user accounts that access internal systems. The password policy requires a minimum password length and the password must meet certain complexity requirements.	(b)(3):6(f),(b)(4)		

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion F - Security for Privacy				
Facebook protects personal information of users against unauthorized access.				
				(b)(3):6(f),(b)(4)
F-9	(b)(3):6(f),(b)(4)			

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion F - Security for Privacy				
Facebook protects personal information of users against unauthorized access.				
		(b)(3):6(f),(b)(4)		

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion F - Security for Privacy				
Facebook protects personal information of users against unauthorized access.				
				(b)(3):6(f),(b)(4)
F-10	(b)(3):6(f),(b)(4)			

pwc

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion F - Security for Privacy				
Facebook protects personal information of users against unauthorized access.				
				(b)(3):6(f),(b)(4)

pwc

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion F - Security for Privacy				
Facebook protects personal information of users against unauthorized access.				
				(b)(3):6(f),(b)(4)

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion F - Security for Privacy				
Facebook protects personal information of users against unauthorized access.				
				(b)(3):6(f),(b)(4)
F-11	(b)(3):6(f),(b)(4)			

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion F - Security for Privacy				
Facebook protects personal information of users against unauthorized access.				
				(b)(3):6(f),(b)(4)
F-12	(b)(3):6(f),(b)(4)			

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion F - Security for Privacy				
Facebook protects personal information of users against unauthorized access.				
	(b)(3):6(f),(b)(4)			
F-13				
F-14				
F-15				

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion F - Security for Privacy				
Facebook protects personal information of users against unauthorized access.				
F-16	(b)(3):6(f),(b)(4)			
F-17				
F-18				

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion F - Security for Privacy				
Facebook protects personal information of users against unauthorized access.				
F-19	(b)(3):6(f),(b)(4)			
F-20				(b)(3):6(f),(b)(4)

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion F - Security for Privacy				
Facebook protects personal information of users against unauthorized access.				
				(b)(3):6(f),(b)(4)
F-21	Facebook's data centers are equipped with environmental controls, including fire suppression systems and fire extinguishers; air conditioning systems; water detection systems; and alternative power supply.	(b)(3):6(f),(b)(4)		

pwc

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion F - Security for Privacy				
Facebook protects personal information of users against unauthorized access.				
F-22	Monitoring of data centers is performed through regularly scheduled reviews of physical and environmental controls as well as periodic reviews of physical security access lists.	(b)(3):6(f),(b)(4)		
F-23	(b)(3):6(f),(b)(4)			
F-24				
F-25	Direct access to user data on Facebook production servers is restricted to authorized personnel.			

pwc

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion G - Third-party developers				
Facebook discloses personal information to third-party developers only for the purposes identified in the notice and with the implicit or explicit consent of the individual.				
G-1	Facebook has the following formal policies in place to ensure that personal information is disclosed only to developers who have agreements with Facebook to protect personal information in a manner consistent with Facebook's privacy program: • Data Use Policy, which informs users about how information is disclosed to applications created by developers when a user connects to those applications. • Facebook's platform policies, which provide specific instructions and details to developers on the handling of user information. • Statement of Rights and Responsibilities, which details specific requirements for handling personal information and the responsibility of the developer to disclose a privacy policy to end users. Non-branded Facebook application developers - Third party developers who leverage on Facebook's Application Programming Interface (API) and tokenization to interact with Facebook users. Facebook Experience (branded) application developers – Third party developer partners who develop Facebook-branded applications as a	(b)(3):6(f),(b)(4)		

pwc

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion G - Third-party developers Facebook discloses personal information to third-party developers only for the purposes identified in the notice and with the implicit or explicit consent of the individual.				
	conduit for interfacing with Facebook services and user data (e.g., Microsoft - "Facebook for Windows"; RIM - "Facebook for Blackberry"). *Refer to Assertion H – Service providers for an outline of the control activities that relate to this type of developer.*			
G-2	Developers must read and sign-off on Facebook's Data Use Policy and Platform Policies during the developer registration process. The developer is responsible for disclosing their own privacy policy to users of their application(s).	(b)(3):6(f),(b)(4)		
G-3	Instagram only: Instagram's "API Terms of Use" and developer site provide specific instructions and details to developers on the handling of user information. Developers must agree to Instagram's terms of service during the developer sign up process, which also details specific requirements for handling personal information and the responsibility of the developer to disclose a privacy policy to its users. Instagram data obtained through the API is consistent with a user's privacy settings and status.			

pwc

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion G - Third-party developers				
Facebook discloses personal information to third-party developers only for the purposes identified in the notice and with the implicit or explicit consent of the individual.				
G-4	(b)(3):6(f),(b)(4)			

pwc

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion H - Service Providers				
Facebook has developed and used reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from the Company and requiring service providers, by contract, to implement and maintain appropriate privacy protections for such covered information.				
H-1	The privacy policies of Facebook and Instagram contain a section that informs users that the information Facebook and Instagram receive may be shared with service organizations when a user signs up for Facebook and Instagram accounts.	(b)(3):6(f),(b)(4)		
H-2	(b)(3):6(f),(b)(4)			
H-3	Facebook Experience application developers (e.g., Microsoft and RIM) must read and sign-off on the Extended API Addendum (the "Addendum"), or other similar agreement, which sets forth the terms and conditions for a developer's adherence to Facebook's Platform			

pwc

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion H - Service Providers				
Facebook has developed and used reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from the Company and requiring service providers, by contract, to implement and maintain appropriate privacy protections for such covered information.				
	Policies, Statement of Rights and Responsibilities and data policies and procedures, which includes consideration of the following privacy-related requirements: • Purpose of Use • Restrictions on Use • Deletion of Data • No Transfer • Updates of Data • Storage			
H-4	(b)(3):6(f),(b)(4)			

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion H - Service Providers				
Facebook has developed and used reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from the Company and requiring service providers, by contract, to implement and maintain appropriate privacy protections for such covered information.				
		(b)(3):6(f),(b)(4)		
H-5	(b)(3):6(f),(b)(4)			

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion H - Service Providers Facebook has developed and used reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from the Company and requiring service providers, by contract, to implement and maintain appropriate privacy protections for such covered information.				
				(b)(3):6(f),(b)(4)

pwc

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion H - Service Providers				
Facebook has developed and used reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from the Company and requiring service providers, by contract, to implement and maintain appropriate privacy protections for such covered information.				
H-6	Service provider contracts may be terminated if Facebook identifies misuse of user information (based on violations of the Statement of Rights and Responsibilities and/or the vendor security policy).	(b)(3):6(f),(b)(4)		

pwc

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion I - On-going Monitoring of the Privacy Program				
Facebook evaluates and adjusts the Company's privacy program in light of the results of monitoring activities, any material changes to the Company's operations or business arrangements, or any other circumstances that the Company knows or has reason to know may have a material impact on the effectiveness of its privacy program.				
I-1	(b)(3):6(f),(b)(4)	(b)(3):6(f),(b)(4)		
I-2	The XFN process ensures that new products and changes to existing products that result in material and/or retroactive changes to the use of information are evaluated to determine whether additional notice or consent from Facebook users is required. Where required, key decisions around the need for additional consent from users are discussed and recommendations are made and implemented by the XFN team.			

pwc

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion I - On-going Monitoring of the Privacy Program				
Facebook evaluates and adjusts the Company's privacy program in light of the results of monitoring activities, any material changes to the Company's operations or business arrangements, or any other circumstances that the Company knows or has reason to know may have a material impact on the effectiveness of its privacy program.				
I-3	(b)(3):6(f),(b)(4)			

pwc

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion I - On-going Monitoring of the Privacy Program				
Facebook evaluates and adjusts the Company's privacy program in light of the results of monitoring activities, any material changes to the Company's operations or business arrangements, or any other circumstances that the Company knows or has reason to know may have a material impact on the effectiveness of its privacy program.				
I-4	(b)(3):6(f),(b)(4)			
I-5				
I-6				

pwc

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion I - On-going Monitoring of the Privacy Program				
Facebook evaluates and adjusts the Company's privacy program in light of the results of monitoring activities, any material changes to the Company's operations or business arrangements, or any other circumstances that the Company knows or has reason to know may have a material impact on the effectiveness of its privacy program.				
	(b)(3):6(f),(b)(4)			

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion I - On-going Monitoring of the Privacy Program				
Facebook evaluates and adjusts the Company's privacy program in light of the results of monitoring activities, any material changes to the Company's operations or business arrangements, or any other circumstances that the Company knows or has reason to know may have a material impact on the effectiveness of its privacy program.				
		(b)(3):6(f),(b)(4)		
I-7	(b)(3):6(f),(b)(4)			
I-8	Facebook's Help Center provides information on how to contact the company with inquiries, complaints and disputes. Users can use e-mail or the "Report" button on the site or in Facebook's products to communicate with Facebook's User Operations (UO) team. The Help Center can be accessed from the "Help" link on any Facebook page.			

pwc

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion I - On-going Monitoring of the Privacy Program				
Facebook evaluates and adjusts the Company's privacy program in light of the results of monitoring activities, any material changes to the Company's operations or business arrangements, or any other circumstances that the Company knows or has reason to know may have a material impact on the effectiveness of its privacy program.				
I-9	(b)(3):6(f),(b)(4)			
I-10				

facebook

Management's Assertion

The management of Facebook represents that as of and for the 180 days ended February 11, 2013 ("the Reporting Period"), in accordance with Parts IV and V of the Agreement Containing Consent Order ("The Order"), with a service date of August 15, 2012, between Facebook, Inc. ("the Company") and the United States of America, acting upon notification and authorization by the Federal Trade Commission ("FTC"), the Company had established and implemented a comprehensive Privacy Program, ("the Facebook Privacy Program"), based on Company specific criteria (described in paragraph two of this assertion); and the privacy controls were 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.

The company specific criteria ("assertions") used as the basis for Facebook's Privacy Program are described below. The below assertions have corresponding controls on pages 21-76.

Assertion A - Responsibility for the Facebook Privacy Program, which is "Facebook has designated an employee or employees to coordinate and be responsible for the privacy program."

Assertion B - Privacy Risk Assessment, which is "Facebook has identified reasonably foreseeable, material risks, both internal and external, that could result in Facebook's unauthorized collection, use, or disclosure of covered information and an assessment of the sufficiency of any safeguards in place to control these risks. This privacy risk assessment includes consideration of risks in areas of relevant operations, including, but not limited to: (1) employee training and management, including training on the requirements of this order, and (2) product design, development, and research."

Assertion C - Privacy and Security Awareness, which is "Facebook has a privacy and security for privacy awareness program in place which is defined and documented in privacy and security for privacy policies. The extent of communications to employees is based on their role and responsibility and may include internal communications through various channels, training, and the Privacy Cross-Functional ("XFN") team process."

Assertion D - Notice, Choice, Consent, Collection and Access, which is "Facebook provides notice about its privacy policies and procedures and terms of service to users which identifies the purposes for which personal information is collected and used, describes the choices available to users, obtains implicit or explicit consent, collects personal information only for the purposes identified in the notices and provides users with access to their personal information for review and update."

Assertion E - Use, Retention, Deletion and Quality, which is "Facebook limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. Facebook retains personal information for as long as necessary to provide services or fulfil the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information. Facebook maintains accurate, complete, and relevant personal information for the purposes identified in the notice."

1601 Willow Road, Menlo Park, California 94025
650.543.4800 – tel 650.543.4801 – fax

Assertion F - Security for Privacy, which is "Facebook protects personal information of users against unauthorized access."

Assertion G - Third-party developers, which is "Facebook discloses personal information to third-party developers only for the purposes identified in the notice and with the implicit or explicit consent of the individual."

Assertion H - Service Providers, which is "Facebook has developed and used reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from the Company and requiring service providers, by contract, to implement and maintain appropriate privacy protections for such covered information."

Assertion I - On-going Monitoring of the Privacy Program, which is "Facebook evaluates and adjusts the Company's privacy program in light of the results of monitoring activities, any material changes to the Company's operations or business arrangements, or any other circumstances that the Company knows or has reason to know may have a material impact on the effectiveness of its privacy program."

Facebook, Inc.

By: _____

Edward Palmieri

Associate General Counsel, Privacy

Facebook, Inc.

By: _____

Daniel Li

Product Counsel

Facebook, Inc.

pwc

Appendix A – Assessment Interviews Summary

The primary Facebook individuals interviewed by PwC, as a part of the above Assessment procedures, include, but are not limited to, those individuals listed in the table below.

Title	Team
Chief Privacy Officer, Product	Privacy
Chief Privacy Officer, Policy	Public Policy
VP & Deputy General Counsel	Legal
Associate General Counsel, Privacy	Legal
Privacy & Product Counsel	Legal
Lead Contracts Manager	Legal
Compliance Associate	Legal
Privacy Program Manager	Identity
Specialist, User Operations	User Operations
Engineering Manager	Engineering
Software Engineer	Engineering
Developer Policy Enforcement Manager	Developer Operations
Platform Operations Analyst	Developer Operations
Chief Security Officer	Security
Manager, Information Security	Security
Policy and Operations Analyst	Security
Security Manager, Incident Response	Security
Mobile Program Manager	Mobile Partner Management
Recruiting Process Manager	Human Resources
US Data Center Operations Director	Infrastructure
Group Technical Program Manager	Infrastructure
Engineering Manager (formerly Instagram Chief Technology Officer)	Instagram - Engineering
User Operations Manager	Instagram - User Operations
Product Manager	Instagram - Product Management