facebook

April 22, 2013

VIA EMAIL AND FEDERAL EXPRESS

James A. Kohm Esq.
Associate Director for the Division of Enforcement
Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, DC 20850

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

Dear Mr. Kohm:

In accordance with Part V of the Decision and Order entered in *In re Facebook*, Docket No. C-4365 (July 27, 2012) ("FTC Order"), enclosed please find a copy of the assessment and report ("Assessment"), prepared by a qualified, objective, independent third-party professional ("Independent Assessor"), examining the sufficiency of the privacy controls that Facebook maintained during the period from August 15, 2012 to February 11, 2013. We are pleased that the Assessment concludes that our Privacy Program was operating effectively throughout the reporting period. This conclusion is based on an exhaustive examination of our program, conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants ("AICPA").

The Facebook Privacy Program

Privacy is central to everything we do at Facebook. Since our founding less than a decade ago, we have worked to develop practices and procedures that ensure that people's personal information is safe, secure, and used in accordance with their sharing settings and choices. Our privacy efforts received a substantial boost in 2011 and 2012, when the Data Protection Commissioner ("DPC") in Ireland, where Facebook's international headquarters is located, undertook the first major governmental review of an internet company's compliance with European data protection law. That review resulted in two comprehensive audit reports that documented Facebook's controls, addressed and rejected a number of misperceptions about how Facebook approaches privacy, and identified areas where we can continue to improve. Facebook Ireland, Ltd., continues to work closely with the DPC to ensure ongoing compliance with EU privacy and data protection law.

The Privacy Program reflected in the attached Assessment built upon our work with the Irish DPC. In developing our program, we went beyond the general requirements set out in Section IV of the FTC Order and leveraged the Generally Accepted Privacy Principles

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

("GAPP"), a comprehensive framework created by the AICPA and Canadian Institute of Chartered Accountants. The GAPP framework is the most comprehensive standard for privacy programs, derived from ten internationally-recognized information principles, including notice, choice and consent, access obligations, and limitations on the use, retention, disposal, and disclosure of personal information. We used the GAPP principles and criteria as a guide in developing our own company-specific privacy assertions and controls. Key features of our program include: (a) the designation of responsible employees, including an experienced Privacy Governance Team, (b) comprehensive awareness and training for all employees, appropriate to their job functions, (c) consideration of privacy issues throughout the development process (i.e., "privacy by design"), (d) robust security for privacy controls, (e) safeguards for Platform developers, (f) screening and contractual obligations for service providers, and (g) assessment and integration of acquisitions.

We also have invested in building innovative tools that provide people with control over the sharing of their information. Our Per-Object Privacy controls and Granular Data Permissions model, for example, enable users to choose, at the time of sharing, the specific audience for each piece of content they share and to have direct visibility into the information available to applications they use. Likewise, our Data Use Policy presents layered content, practical headings and screenshots to help users understand how the information they provide is used and shared. We have strengthened existing controls, like Activity Log, which allows people to sort, review, delete or hide the things they post on Facebook. In addition, we continue to launch new controls, such as our privacy shortcuts, which are located at the top of most pages on Facebook and allow users to quickly access key settings and easily visit their main settings page. We believe these tools demonstrate our commitment to achieving the balance users want between sharing information quickly and easily while maintaining appropriate privacy and control.

Independent Assessment

The attached report is a comprehensive assessment of our Privacy Program. It documents our assertions and controls and, for each, describes the testing procedures used to gauge whether the control was operating effectively. The Assessment also identifies areas where control design and/or operating effectiveness can continue to improve. This report follows fifteen weeks of intense on-site work by the Independent Assessor at Facebook's headquarters in Menlo Park. As part of that process, the Independent Assessor engaged in over 65 in-person meetings with key individuals involved in our program (e.g., the Chief Security Officer, the Chief Privacy Officer, Product, the Chief Privacy Officer, Policy) and examined a wide range of materials—including, among other things, written policies and procedures and representative data sets. The Independent Assessor was comprised of thirteen team members with cross-disciplinary experience in privacy, assessment, and technology and led by a partner with decades of experience in the area of data protection and privacy. Among the team were Certified Information Privacy Professionals, Certified Information Systems Auditors, and Certified Public Accountants. In addition, individuals with specialized experience in the Independent Assessor's

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

quality assurance and risk management practices were consulted and brought into the assessment as needed.

At Facebook, we put privacy at the core of our mission. The attached Assessment reaffirms our commitment to implementing meaningful and effective privacy and security controls. While the Assessment reflects our years of privacy and security innovation and expertise, we view this commitment as ongoing. We will continue to work to meet the changing and evolving needs of our users and to put user privacy and security at the center of everything we do. The Privacy Program – and the Assessment – provide a clear, positive framework for Facebook to move forward in this pursuit.

* * *

Request for Confidentiality

Pursuant to 16 C.F.R. § 4.10(a)(2), we have enclosed two versions of the Assessment – a confidential version that contains highly confidential Facebook and Independent Assessor commercial and trade secret information, and a non-confidential version that redacts such information.

The redacted text contains detailed trade secret information regarding the design and testing of the Facebook Privacy Program. We believe that release of the redacted information would place user information at risk, as it would reveal detailed information regarding the specific strengths and possible limitations of the Facebook Privacy Program to hackers and other third parties that may attempt to infiltrate our system in the future. Furthermore, public disclosure of this information would place both Facebook and the Independent Assessor at a competitive disadvantage vis-à-vis competitors, who could use the information to mimic Facebook's industry-leading development processes or the Independent Assessor's proprietary testing protocols.

For these reasons, we respectfully request that the Commission treat the redacted information as confidential and not subject to the Freedom of Information Act, pursuant to 5 U.S.C. § 552(b)(4).

* * *

We hope that you find the information above and the enclosed Assessment informative. Please do not hesitate to contact us should you have any questions.

Sincerely,

Michael Richter
Chief Privacy Officer, Product

Erin Egan
Chief Privacy Officer, Policy

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

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

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 LLP

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.

facebook

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

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.

facebook

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

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

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

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

pwc

Independence

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

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

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

PwC Assessment Process Overview

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

pwc

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

pwc

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

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.

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

pwc

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

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

pwc

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

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

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

pwc

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

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

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

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

pwc

pwc

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

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

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

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

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

pwc

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

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

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

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

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

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

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

pwc

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

pwc

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

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

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

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

pwc

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

pwc

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

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

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

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

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

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

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

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

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

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

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

pwc

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

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

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

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

pwc

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

pwc

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

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

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

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

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

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

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

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

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

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

pwc

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

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

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