Independent Assessor's Report on Facebook's Privacy Program

Biennial Report

For the period February 12, 2013 to February 11, 2015

Table of Contents

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 independent assessment.

As described on pages 6-14, 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 15-18, 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 two years ended February 11, 2015, 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 two years ended February 11, 2015 (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 ("the Facebook Privacy Program"), as described in Management's Assertion, 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.

Note that during the Reporting Period, Facebook made acquisitions. As part of its acquisition process, the Company assesses whether the operations and technology of an acquired entity will be integrated with the Company or if it will remain independently operated. As the scope of the Order requires a comprehensive privacy program for Facebook, Inc., any independently operated affiliates were not included in the assessment of the Facebook Privacy Program. The products and services of Facebook, Inc., subject to the scope and assessment, are those generally available through Facebook's websites, facebook.com or m.facebook.com and/or Facebook's mobile applications.

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 two years ended February 11, 2015, based upon the Facebook Privacy Program set forth in Management's Assertion.

pwc

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

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 13, 2015

Facebook's Privacy Program Overview

Introduction

Facebook is a publicly traded U.S. company headquartered in Menlo Park, California. Established in February 2004, Facebook's mission is to give people the power to share and make the world more open and connected. People use Facebook to stay connected with friends and family, to discover what's going on in the world, and to share and express what matters to them. In doing so, people entrust Facebook with information when they use our services.

To ensure we maintain people's trust, Facebook has integrated privacy considerations into its product development and business plans since its inception. Facebook formalized its privacy objectives, and the procedures it has implemented to achieve them, in 2012. And, as Facebook has grown and matured, so has its Privacy Program – ensuring that the program remains relevant and effective. As part of that program, Facebook continually evaluates people's experiences using its services. For example, Facebook recently updated its Data Policy to make it easier for people to understand, consistent with industry standards, thus promoting the balance between simple disclosures and the expression of key information about data practices.

The Privacy Program has also resulted in countless privacy-friendly product features, privacy and security training, and other privacy tools. For example, Facebook launched Privacy Basics alongside the new Data Policy. Privacy Basics offers interactive guides to answer commonly asked questions about how people can control their information on Facebook. Facebook also launched the Privacy Check-up Tool, which helps people review and control who they are sharing with via status updates, on their profile, or when they use apps on Facebook's Platform.

This Privacy Program Overview describes the scope and background of Facebook's formal Privacy Program and the procedures developed to ensure Facebook achieves its privacy objectives. The accompanying report submitted by our independent assessor, PricewaterhouseCoopers LLP ("PwC"), provides additional details on these controls and the results of the rigorous tests performed in connection with this assessment.

Background and Scope of Privacy Program

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's Privacy Program is defined by nine assertions inspired by 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"). In particular, Facebook's assertions include the following:

A. **Responsibility for the Facebook Privacy Program:** Facebook has designated an employee or employees to coordinate and be responsible for the Privacy Program.

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.
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.
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.
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.
F. **Security for Privacy:** Facebook protects personal information of users against unauthorized access.
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.
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.
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.

As discussed further below, *see infra* at Test Environment, Facebook has implemented numerous procedures ("controls") to achieve and evidence these objectives.

Although the Order limits the scope of this assessment to evaluating the practices of Facebook, Inc., achieving the objectives of the Privacy Program involves taking a hard look at the privacy practices of any entities acquired by Facebook. Facebook's acquisitions run the gamut, ranging from businesses whose employees and operations become fully integrated with Facebook, Inc. to operational units that continue to run independently. In any event, Facebook regularly notifies the FTC of acquisitions.

As part of the acquisition process, Facebook assesses whether its integration of acquired companies effects any material change to Facebook's operations or business arrangements or has a material impact on the effectiveness of Facebook's Privacy Program. Where an acquisition effects a change to Facebook operations or impacts the effectiveness of its Privacy Program, Facebook adjusts its Privacy Program to ensure the program achieves its objectives; specifically, its objectives (1) to address privacy risks related to the development and management of new and existing products and services for Facebook consumers and (2) to protect the privacy and confidentiality of information from or about an individual Facebook consumer.

In practice this means that Facebook regularly assesses its Privacy Program and incorporates acquisitions and other affiliates into the formal program controls where appropriate. (b)(3):6(f),(b)(4)

(b)(3):6(f),(b)(4) Second, Facebook's Privacy Program stakeholders periodically review and adjust the Privacy Program, including relevant privacy policies and procedures, in light of material changes in operations, business arrangements or other internal or external factors. For example, Facebook holds an annual privacy summit ("Privacy Summit") that includes key representatives from the Privacy Cross-functional Team ("Privacy XFN") responsible for the product development process. *See infra* at Test Environment Parts B & I. Attendees of the Privacy Summit also review and update the privacy risk assessment ("Risk Assessment"), focusing on significant material risks identified by the Privacy Governance Team responsible for coordinating Facebook's Privacy Program. *See id.* at Test Environment Parts A, B, & I. The Privacy XFN team considers the sufficiency of existing controls in addressing current and future risks and makes recommendations for changes to the Privacy Program.

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

Test Environment

Facebook has identified 61 controls to support the above-listed assertions. This section provides a high-level summary of some of the processes Facebook implements to ensure that it achieves each of its privacy objectives.

A. Responsibility for the Facebook Privacy Program

Facebook has designated a team of employees who are directly responsible for the Facebook Privacy Program (the "Privacy Governance Team"). The team members include the Chief Privacy Officer, Policy; Chief Privacy Officer, Product; Chief Security Officer; Deputy General Counsel; Associate General Counsel, Privacy and Regulatory; Associate General Counsel, Privacy and Product; Associate General Counsel, Advertising and Product; and the Head of Data Protection for Facebook Ireland. The Privacy Governance Team and many employees (including engineers, product managers, security experts (discussed further *infra* at Part F), 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. The Privacy Governance Team is also responsible for establishing, communicating and monitoring relevant control policies and procedures. These policies and procedures are reviewed periodically and updated as needed. Of particular note are the Privacy Program Managers. The Privacy Program Managers work closely with the product organization and are 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. In addition to working closely with the Privacy Program Managers, the Privacy Legal and Policy teams work closely with relevant stakeholders throughout Facebook to regularly (a) assess compliance with established privacy controls; (b) improve design and operation of privacy controls; and (c) evaluate and document privacy risks, as discussed further below.

B. Privacy Risk Assessment

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 consider risks in each relevant area of Facebook's operation, including governance, product design, engineering (including product development and research), community operations (including third-party developers), advertising, service providers, employee awareness and training, employee management, and security for privacy. The Privacy Governance Team works with stakeholders responsible for each of these areas of operations to identify reasonably foreseeable, material risks, both internal and external, that could result in the unauthorized collection, use or disclosure of covered information. 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.

Facebook has implemented numerous avenues through which relevant stakeholders can identify, assess, and remediate risk. For example, members of the Privacy XFN Team assess risks and controls on an on-going basis through focused subject-matter-specific meetings and weekly intra- and inter-team meetings. Likewise, 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. This cross-functional collaboration allows Facebook to continually evaluate and adjust the Privacy Program in light of the results of testing and monitoring of the program as well as other relevant circumstances.

Above and beyond our privacy assessment, Facebook retains an independent third-party assessor to conduct a controls assessment based on the AICPA's AT 101 standard. The annual assessment, conducted under the direction of Facebook's Information Security team, covers the security and confidentiality Trust Service Principles, culminating in the issuance of a Service Organization Controls 3 ("SOC3") report for Facebook's ads systems. The Information Security team has placed into operation a risk assessment process to identify and manage risks that affect Facebook's ability to achieve its defined security and confidentiality objectives for its platforms.

C. Privacy and Security (for Privacy) Awareness

Facebook communicates Privacy and Security awareness matters to new and existing employees and tailors such communications according to applicable role and responsibility. For example, all new employees must complete a robust privacy and security awareness training upon hire, while all existing employees are required to complete the privacy training periodically. This training covers, among other things, (1) an overview of applicable privacy laws and other privacy commitments (such as Facebook's obligations under the Consent Order); (2) Facebook's policies with respect to accessing data belonging to people who use Facebook; (3) common security vulnerabilities and strategies for avoiding them; (4) the importance of privacy by design; and (5) resources personnel can contact for help. Facebook employees are quizzed on their understanding of Facebook's privacy practices during the training, and are not allowed to proceed unless and until they receive a passing score.

Above and beyond the controls tested as part of the privacy assessment, Facebook targets additional training to key stakeholders with access to covered information. For example, as part of its regular training for new product managers, Facebook trains project managers about the Privacy Program and key privacy considerations during the product development cycle. In this training, representatives from the Privacy XFN Team present to the product 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 a further example, engineers at Facebook spend their first six weeks in boot camp, an immersive, cross-functional orientation program. During boot camp, 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., community 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 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.

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

D. Notice, Choice, Consent, Collection, and Access

Facebook notifies people about its privacy policies and implements robust procedures to ensure that it complies with the choice, collection, and access principles described therein. More specifically, Facebook's Data Policy – which all users must agree to upon signing up to receive the service and which is consistently available and readily apparent to people across platforms – describes the types of data collected, the purposes for which it is used, and the parties with whom it is shared, among other things. Facebook recently amended the Data Policy to make it easier for people to read and understand, and implemented Privacy Basics and new content in the Facebook Help Center that educates people about how to protect their privacy on Facebook.

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

Facebook also offers multiple tools that help people to access, delete, change, and protect information as described in the Data Policy. For example, Facebook allows users to select

an audience for their content through various tools such as account settings and/or in-line privacy controls. Likewise, Facebook's Activity Log allows users to review, update, delete or correct information they have previously provided while the Download Your Information tool allows users to create a downloadable archive of their activity.

E. Use, Retention, Deletion, and Quality

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

Facebook also minimizes risk associated with data stored on Facebook infrastructure by implementing and enforcing procedures to destroy and/or wipe servers, drives, and laptops before they leave Facebook's custody.

F. 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 and supported by a dedicated Security Team. As mentioned above, the Chief Security Officer 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.

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

Policies within each of these areas create the overall framework that Facebook uses to secure systems across the environment, which are tested and enforced across platforms. As described above, *see supra* at Part B, Facebook personnel receive training on these policies commensurate with their responsibilities and roles.

G. Third-Party Developers

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 settings and Granular Data Permissions ("GDP") process allow users to control the transfer of Facebook user information to third-party applications.

H. 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.

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

Facebook also has a contract policy (the "Contract Policy"), which governs the review, approval, and execution of contracts for Facebook

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

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

I. On-Going Monitoring of the Privacy Program

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. 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.

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

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.

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 with more than 19 years of experience providing professional services led the engagement and was supported by a partner with more than 25 years of experience providing professional services. The assessment was performed by an experienced team of over fifteen 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"), Certified Information Privacy Manager ("CIPM") 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 were performed in four phases over the two year period, incurring over 5,700 hours. The fieldwork was primarily performed at Facebook's headquarters in Menlo Park, CA.

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 two years ended February 11, 2015.

PwC designed and performed test procedures to evaluate the design effectiveness and operating effectiveness of the control activities implemented by Facebook for the two years ended February 11, 2015.

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. PwC 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 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 22-57 of this document.

Over the course of the reporting period, PwC performed procedures that included interviewing individuals from Privacy, Legal, Identity, Marketing, Security, Community Operations, Developer Operations, Engineering, Infrastructure, Mobile Partner Management, and Human Resources. Test plans for each control activity tested are also included on pages 22-57 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 58-59. 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 22-57, 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 58-59 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 6-14, 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 22-23 (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 25-50 (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 51-52 (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 53-57 (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.

pwc

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.

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. Facebook has defined roles, responsibilities and qualifications for key positions supporting the privacy team, including the Privacy Governance Team (responsible for coordinating Facebook's Privacy Program) and the Privacy Cross-functional Team ("Privacy XFN") (responsible for the product development process).	(b)(3):6(f),(b)(4)		

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-2	Facebook has designated a team of employees who are directly responsible for the Information Security Program (the "Security Team") which closely supports the privacy program. Facebook's Chief Security Officer leads the information security team. Facebook has defined roles and responsibilities for key positions supporting the information security team (responsible for coordinating Facebook's Security Program).	(b)(3):6(f),(b)(4)		

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 ("Privacy Summit") that includes key representatives from the Privacy XFN. Attendees of the Annual Summit review and update the privacy risk assessment ("Risk Assessment"), focusing on significant material risks identified by the Privacy Governance Team. Risks are evaluated in light of changing internal and external threats, changes in operations, and changes in laws and regulations. The sufficiency of existing controls in addressing current and future risks is considered; recommendations are escalated and changes to the Privacy Program are considered.	(b)(3):6(f),(b)(4)		

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 has defined and documented privacy policies, which govern its relationship with users and others who interact with Facebook. The following policies are documented and made available through various forms (e.g., on the website / mobile application / internal Wiki, for third-party applications, and on all in-scope platforms and products (e.g., Android / iOS). • Data Policy (previously titled Data Use Policy ("DUP")) • Statement of Rights and Responsibilities ("Terms") • Platform Policy (Third-Party Developer Policies) The topics covered within these policies include the following: • Notice • Choice and consent • Collection • Type and source of information collected • Use, retention, and deletion • Access • Disclosure to third parties • Security for privacy • Quality • Monitoring and enforcement	(b)(3):6(f),(b)(4)		

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-2	(b)(3):6(f),(b)(4)			

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

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-5	(b)(3):6(f),(b)(4)			

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)			

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)			

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

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)			

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-7	(b)(3):6(f),(b)(4)			
C-8	Facebook has a Privacy 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 and that key privacy decisions are implemented for the product.	(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.				
D-1	The privacy policies for Facebook 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	At the time of account creation, a user consents to sharing certain personal information that is part of their "Public Profile," including gender, username and user ID (account number), profile picture, cover photo,			

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.				
	network(s), age range, language, and country. By clicking on the "Sign Up" button after entering this information, the user provides explicit consent at the time of account creation through agreement to the Terms and acknowledgment of the Data Policy. The user provides consent for user information to be collected and chooses to share the information with Facebook and to make certain information public (i.e., the Public Profile). Upon sign-up, the user consents to not provide any false personal information on Facebook, as well as the responsibility to keep such information accurate and up-to-date. 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.	(b)(3):6(f),(b)(4)		
D-3	Facebook users can often control (e.g., via in-line privacy settings and account settings) the audience for their content (e.g., status updates, photos, posts). On most platforms, a user is able to select a specific audience at the time of posting. Facebook does not change the audience for a piece of content without permission from the poster.			

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.				
	Note: This does not include instances where third parties control the audience, such as a user's comment on a public event.	(b)(3):6(f),(b)(4)		
D-4	Facebook has a Privacy 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 and that key privacy decisions are implemented for the product.			
D-5	Facebook users and non-users can access and update their personal information through various methods.			

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-6	Facebook does not deny active users access to their personal information through Facebook products and platforms, unless the user violates Facebook's policies. Users may appeal this process by contacting Facebook.			

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 Data Policy and Terms address 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				

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.				
	(b)(3):6(f),(b)(4)			
E-7				
E-8				
E-9				

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	(b)(3):6(f),(b)(4)			
F-2				
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)	(b)(3):6(f),(b)(4)		
F-5				
F-6	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.			
F-7	(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.				
F-8	(b)(3):6(f),(b)(4)			
F-9				
F-10				

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-11	(b)(3):6(f),(b)(4)			
F-12				
F-13				(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-14				
F-15				
F-16				

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-17	Facebook has procedures in place to restrict access to its data centers to only authorized employees. Access lists to data centers are reviewed by respective data center managers or delegates on a periodic basis.	(b)(3):6(f),(b)(4)		
F-18	(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.				
F-19	(b)(3):6(f),(b)(4)			

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 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. • Terms, which detail specific requirements for handling personal information and the responsibility of the developer to disclose a privacy policy to end users.	(b)(3):6(f),(b)(4)		
G-2	Facebook requires developers who access public APIs to agree to Facebook's Data Policy, Terms, and Platform Policy, which include consideration of privacy-related requirements such as: • Purpose of Use • Restrictions on Use • Deletion of Data • No Transfer • Updates of Data • Storage			

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-3	Management has implemented mechanisms to ensure that Facebook obtains consent from users prior to disclosing non-public personal information to third-party developers. Third party developers are limited to accessing user information based on an appropriate permission list consented to by the user.	(b)(3):6(f),(b)(4)		
G-4	(b)(3):6(f),(b)(4)			
G-5	Facebook requires developers who access non-public APIs to agree to Facebook's Data Use Policy, Terms, and Platform Policies, which include privacy-related requirements such as: • Purpose of Use • Restrictions on Use • Deletion of Data • Transfer • Storage In addition, each non-public API request must be specifically approved by an authorized Facebook employee.			

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	Facebook's Data Policy contains a section that informs users that the information Facebook receives may be shared with service organizations when a user signs up for a Facebook account.	(b)(3):6(f),(b)(4)		
H-2	(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.				
H-3	(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.				
I-1	(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.				
I-2	(b)(3):6(f),(b)(4)			
I-3				

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)	(b)(3):6(f),(b)(4)		
I-4				
I-5	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 Community Operations team. The Help Center can be accessed from the "Help" link on any Facebook page.			

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-6	(b)(3):6(f),(b)(4)			
I-7				

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)	(b)(3):6(f),(b)(4)		
I-8	Facebook holds an annual privacy summit ("Privacy Summit") that includes key representatives from the Privacy XFN. Attendees of the Annual Summit review and update the privacy risk assessment ("Risk Assessment"), focusing on significant material risks identified by the Privacy Governance Team. Risks are evaluated in light of changing internal and external threats, changes in operations, and changes in laws and regulations. The sufficiency of existing controls in addressing current and future risks is considered; recommendations are escalated and changes to the Privacy Program are considered.			

facebook

Management's Assertion

The management of Facebook represents that as of and for the two years ended February 11, 2015 ("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. Note that during the Reporting Period, Facebook made acquisitions. As part of its acquisition process, the Company assesses whether the operations and technology of an acquired entity will be integrated with the Company or if it will remain independently operated. As the scope of the Order requires a comprehensive privacy program for Facebook, Inc., any independently operated affiliates were not included in the assessment of the Facebook Privacy Program. The products and services of Facebook, Inc., subject to the scope and assessment, are those generally available through Facebook's websites, facebook.com or m.facebook.com and/or Facebook's mobile applications.

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 22-57.

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 (for Privacy) 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."

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

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."

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."

Furthermore, the Company represents that for the Reporting Period, Facebook's Privacy Program contains controls and procedures appropriate to its size and complexity, the nature and scope of its activities, and the sensitivity of the covered information.

Facebook, Inc.

By: _____

Edward Palmieri

Director, Associate General Counsel – Privacy & Regulatory

Facebook, Inc.

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

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
Director, Associate General Counsel - Privacy & Regulatory	Legal
Lead Privacy Counsel	Legal
Lead Contracts Manager	Legal
Program Manager, Privacy and Data Protection	Legal
Lead Litigation Paralegal	Legal
Head of Privacy Program	Marketing
Content Strategy, Marketing	Marketing
Privacy Program Manager	Identity
Specialist, User Operations	Community Operations
Business Operations Manager	Community Operations
Engineering Manager	Engineering
Software Engineer	Engineering
Care Engineering	Engineering
Build Engineer	Engineering
Mobile Release Engineering	Engineering
Tools and Automation Specialist	Engineering
Developer Policy Enforcement Manager	Developer Operations
Platform Operations Analyst	Developer Operations
Chief Security Officer	Security
Director, Information Security Policy and Risk	Security
Information Security Risk Manager	Security
Risk & Compliance Analyst	Security
Policy and Operations Analyst	Security

Title	Team
Security Manager, Incident Response	Security
Mobile Program Manager	Mobile Partner Management
Recruiting Process Manager	Human Resources
HR Specialist	Human Resources
Lead, People Service, L&D Benefits Ops	Human Resources
Peeps Partner Lead	Human Resources
US Data Center Operations Director	Infrastructure
Group Technical Program Manager	Infrastructure
Logistics Program Manager, Asset Management	Infrastructure
Product Manager	Product