

Independent Assessor's Report on Google Inc.'s Privacy Program

Biennial Assessment Report

For the period April 26, 2014
through April 25, 2016

June 24, 2016

This report (Report) contains Promontory Financial Group, LLC (Promontory) proprietary information that shall be protected from disclosure outside of the U.S. Government in accordance with the U.S. Trade Secrets Act and Exemption 4 of the U.S. Freedom of Information Act (FOIA). The Report constitutes and reflects work performed or information obtained by Promontory in our capacity as independent assessor for Google Inc. for the purpose of Google Inc.'s Order. The Report contains proprietary information, trade secrets, and confidential commercial information of Promontory and Google Inc. that is confidential, and we expressly reserve all rights with respect to disclosures to third parties. Accordingly, we request confidential treatment under FOIA, the U.S. Trade Secrets Act, or similar laws and regulations when requests are made for the Report or information contained therein or any documents created by the United States Federal Trade Commission (FTC) containing information derived from the Report. We further request that written notice be given to Promontory and Google Inc. before distribution of the information in the Report (or copies thereof) to others, including any other governmental agency, to afford Promontory and Google Inc. the right to assert objections and defenses to the release of the information as permitted under FOIA or other similar applicable law or regulation, except when such distribution is already required by law or regulation. This Report is intended solely for the information and use of the management of Google Inc. and the FTC and is not intended to be and should not be used by anyone other than these specified parties.

Promontory Financial Group, LLC
801 17th Street, NW, Suite 1100 | Washington, DC 20006
+1 202 384 1200 | promontory.com



HIGHLY CONFIDENTIAL

Contents

I.	Introduction	1
II.	Report of Independent Assessor	3
III.	Assessment Requirements Under Part IV of the Order	5
IV.	Assessment Approach	7
	A. Overview	7
	B. Independence	9
	C. Assessor Qualifications	9
V.	Google's Privacy Program Overview	10
	A. Company Overview	10
	B. Google Privacy Program Scope	10
	C. Roles and Responsibilities	12
	D. Privacy Risk Assessment	14
	E. Controls and Procedures	16
	F. Monitoring and Testing	21
	G. Service Provider Oversight	22
	H. Program Evaluation and Adjustment	24
VI.	The Google Privacy Program: Assertions, Controls, Assessment Activities, and Assessment Results	25
VII.	Management's Assertion	42
VIII.	Appendix A – Assessment Interviews Summary	44
IX.	Appendix B – Google Teams Providing Evidence or Input	45
X.	Appendix C – Types of Evidence Reviewed	46

I. Introduction

Effective October 28, 2011, Google Inc. (Google or the Company) entered into Agreement Containing Consent Order File No: 1023136 (Order) with the U.S. Federal Trade Commission (FTC).

Part III of the Order requires Google 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. As defined by the Order, "covered information" means information that Google collects from or about an individual, including, but not limited to, an individual's: (a) first and last name; (b) home or other physical address, including street name and city or town; (c) email address or other online contact information, such as a user identifier or screen name; (d) persistent identifier, such as IP address; (e) telephone number, including home telephone number and mobile telephone number; (f) list of contacts; (g) physical location; or any other information from or about an individual consumer that is combined with (a) through (g) above.

Part IV of the Order requires Google to obtain biennial assessments (Assessments) of its privacy program from a "qualified, objective, independent third-party professional" (Assessor) "who uses procedures and standards generally accepted in the profession." The Assessor must then provide a report detailing the Assessment results (Report). Google retained Promontory Financial Group, LLC (Promontory or we) to perform this Assessment for the biennial period beginning April 26, 2014, and ending April 25, 2016 (the Reporting Period).

Similar to previous Assessments, Google's management set forth Company-specific criteria (Assertions) that described, at a high level, the privacy controls that Google implemented and maintained during the Reporting Period to meet or exceed the protections required by Part III of the Order. These Assertions, which are unchanged from the previous Assessment, constitute the basis of the Google Privacy Program. Google's management also set forth written descriptions of the corresponding privacy controls that support the Assertions. Google set forth 35 privacy controls to support the seven Assertions.

GOOGLE PRIVACY PROGRAM							
ASSERTION #	1	2	3	4	5	6	7
# CORRESPONDING PRIVACY CONTROLS	3	3	3	14	4	3	5

This Report presents the final results of the Assessment for the Reporting Period. In section II, we provide a summary of Promontory's review methodology and Promontory's conclusions resulting from the Assessment. In section III, we list the Assessment requirements under Part IV of the Order and summarize our efforts to meet each of those requirements. In section IV, we describe in further detail



Promontory's Assessment approach, actions to maintain independence throughout the Assessment, and qualifications to serve as the Assessor. In section V, we describe our observations of Google's privacy controls and explain how these controls met or exceeded the requirements of Part III of the Order. In section VI, we summarize our Assessment activities and results for each of the Assertions and corresponding privacy controls. Finally, section VII contains Management's Assertion, which constitutes Google management's representation of the Company's compliance with the Order...

II. Report of Independent Assessor

Introduction We have examined Google Management's Assertion contained on page 42 of this Report, which states, in part, that:

- The Company had established and implemented a comprehensive privacy program, based on Company-specific criteria.
- The Company'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.
- The privacy controls within the Google Privacy Program are appropriate to Google's size and complexity, the nature and scope of its activities, and the sensitivity of the covered information.

The Company is responsible for the content of Management's Assertion, the Assertions, and the corresponding privacy controls. Our responsibility is to express our conclusions with respect to the requirements of the Order based on our review.

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

Conclusions Promontory concludes that, during the Reporting Period, Google's privacy controls were appropriate to Google's size and complexity, the nature and scope of Google's activities, and the sensitivity of the covered information. Promontory further concludes that Google's privacy controls operated with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls so operated throughout the Reporting Period, in all material respects as of

and for the two years ended April 25, 2016, based upon the Google Privacy Program set forth in the Assertions. Promontory did not observe during the Assessment any exceptions to the Assertions and corresponding privacy controls provided by Google.

Use of this Report

This Report is intended solely for the information and use of the management of Google and the FTC and is not intended to be and should not be used by anyone other than these specified parties.

III. Assessment Requirements Under Part IV of the Order

In this section, we describe how the Assessment met the requirements contained in Part IV of the Order (items A through D). According to the Order, each Assessment shall:¹

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

In section VI of this Report, we have listed the privacy controls Google implemented and maintained during the Reporting Period to meet or exceed the protections required by Part III of the Order. The Assertions for this Assessment are unchanged from the previous Assessment. Google identified 35 controls to support the seven Assertions. In section VI, we provide a description of Promontory's test procedures to assess the effectiveness of Google's privacy controls as well as the test results.

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

In section V of this Report, we provide a summary of the Google Privacy Program and the privacy controls we observed during the Assessment. These controls include:

- Privacy Program staffing and subject matter expertise;
- Employee privacy training and awareness;
- Internal and external policies, procedures, and guidelines;
- Privacy risk assessment activities;
- Product launch reviews for privacy considerations;
- Privacy code audits;
- End user privacy tools and settings;
- Complaint and feedback processes and mechanisms;
- Periodic internal and external Privacy Program assessments;
- Coordination with, and support of, the Google information security program;
- Third party service provider oversight;
- Incident reporting and response procedures; and
- Safe Harbor certification.

Based on our observations and testing, as further described in sections V and VI, we conclude that the foregoing controls were appropriate to Google's size and complexity, the nature and scope of Google's activities, and the sensitivity of the covered information during the Reporting Period.

¹ We have made two non-substantive changes to the original Order language for readability: (1) we have changed "respondent" to "Google" and (2) we have changed "this order" to "the Order".

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

In section V, we describe the Google privacy controls that have been implemented and explain how these controls met or exceeded the protections required by Part III 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.

In section II above, we provided our conclusion that Google's privacy controls were operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls so operated throughout the Reporting Period, in all material respects, based upon the Assertions and corresponding privacy controls. We based this conclusion on our observations and test results during the Assessment, which we describe further in sections V and VI of this Report.

IV. Assessment Approach

The following is a description of Promontory's Assessment approach, actions to maintain independence, and Assessor qualifications.

A. Overview

To evaluate the privacy controls that Google implemented and maintained 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, Promontory developed and performed the following procedures:

- **Inquiry:** (b)(3):6(f),(b)(4)
(b)(3):6(f),(b)(4)
- **Observation and Examination:** (b)(3):6(f),(b)(4)
(b)(3):6(f),(b)(4)
(b)(3):6(f),(b)(4)
- **Sampling and Testing:** (b)(3):6(f),(b)(4)
(b)(3):6(f),(b)(4)

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

INQUIRY

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

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

OBSERVATION

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

EXAMINATION

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

SAMPLING AND TESTING

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

B. Independence

Promontory acted as an independent third-party professional in conducting the Assessment. Throughout this engagement, Promontory sought to avoid *actual* conflicts of interest that could impair our ability to provide Google with Promontory's independent professional judgment and sought to avoid any *perceived* conflicts that could cause others to question Promontory's independence. Promontory also established an internal advisory team, independent of Promontory's core Assessment team, to provide ongoing oversight, review, and input into the Assessment methodology and execution.

Although Promontory has, in our capacity as the Assessor, consulted with Google and its employees and representatives, as necessary, during the course of the Assessment, we have exercised our own best professional judgment with respect to the methodology and our ultimate findings and conclusions.

C. Assessor Qualifications

Promontory is a strategy, risk management, and regulatory compliance consulting firm founded in 2001. Promontory professionals include former senior regulators, executives, lawyers, auditors, and advisers. We have assisted clients located in more than 50 countries from offices in North America, Europe, Asia, Australia, and the Middle East.

Promontory formed its Privacy and Data Protection team in 2010. Since that time, we have evaluated privacy and data protection practices, policies and relevant regulations in more than 70 countries. Our team members have served as chief privacy officers, chief information security officers, regulators, lawyers, and consultants.

The leads of Promontory's global Privacy and Data Protection and Consumer Protection practice areas, both of whom bring direct experience as former auditors, led this Assessment. Our team included the head of Promontory's U.S. Privacy and Data Protection practice area and other members of the practice. Our team included Certified Information Privacy Professionals (CIPPs) and had expertise and experience conducting privacy, compliance, and risk assessments.

V. Google's Privacy Program Overview

In this section, we provide our observations regarding the Google Privacy Program, derived from onsite interviews, document review, control testing, and publicly available information. Specifically, we set forth the specific privacy controls that Google implemented and maintained during the Reporting Period and explain how these privacy controls were appropriate to Google's size and complexity, the nature and scope of Google's activities, and the sensitivity of the covered information. We describe the privacy controls that aligned with Assertions 1 through 7 in sub-sections B through H, respectively. Where applicable, we explain how the privacy controls that were implemented met or exceeded the protections required by Part III of the Order.

A. Company Overview

Google was founded in 1998 by Larry Page and Sergey Brin. Since its inception, Google has expanded beyond its core Internet search engine to offer a variety of services, including, but not limited to:

- AdWords and AdSense, proprietary advertising services;
- Gmail, an email service;
- Google Maps, a map and navigational product;
- Google Apps, including Google Docs, Google Sheets, and Google Drive;
- Blogger, a blog-publishing service;
- Google Chrome, a web browser;
- Android, a mobile operating system;
- Google Wallet, a peer-to-peer payments service;
- YouTube, a video sharing service; and
- Google+, a social network.

Google became a publicly traded company on August 18, 2004. The Company now has offices in more than 40 countries and provides products and services in over 130 languages to Google users all over the world. It is headquartered in Mountain View, California and employs more than 50,000 people.

During this Reporting Period, Google announced plans to create a new public holding company, Alphabet Inc. (Alphabet), by implementing a holding company reorganization. Alphabet became the publicly traded entity, and Google became a wholly owned subsidiary of Alphabet. During the Reporting Period, Alphabet's operations all remained a part of Google.

B. Google Privacy Program Scope

In this sub-section, we describe Google's privacy controls relating to Management Assertion 1: "Google has implemented and maintains a comprehensive privacy program, which is documented in written policies and procedures."

INTERNAL PRIVACY POLICIES

The Google Privacy Program is responsible for user and employee privacy at Google Inc. and its subsidiaries. Google describes privacy requirements for employees through a set of core internal privacy policies, available to all Google employees through the Company intranet. All employees are required to comply with these policies, and the Company takes disciplinary action for employees who do not comply. The policies cover the following privacy and data protection topics, among others:

- Google's Privacy Principles (see below);
- Google employees' responsibilities with respect to privacy and data protection;
- Requirements for creating privacy policies, including those related to policy content and structure, and policy non-compliance;
- Data classification, as well as the requirements for accessing, sharing, and storing user data;
- Privacy incident reporting requirements and incident response roles and responsibilities;
- Anonymization techniques;
- User data retention and deletion tools, timeframes, and requirements;
- Requirements for providing notice and obtaining user consent; and
- Standards and policies for the use of cookies and other client-side management mechanisms in Google products.

Google's Privacy Policy Advisory Committee is responsible for developing, reviewing, and updating all privacy policies. The committee includes representatives from, but not limited to, Privacy Engineering, Privacy Incident Response, Ethics and Compliance, and Privacy Legal. The committee periodically reviews and updates, as necessary, each privacy policy.

PRIVACY PRINCIPLES

Google has established five core privacy principles (the Privacy Principles):

1. Use information to provide our users with valuable products and services.
2. Develop products that reflect strong privacy standards and practices.
3. Make the collection of personal information transparent.
4. Give users meaningful choices to protect their privacy.
5. Be a responsible steward of the information we hold.

Google shares these Privacy Principles internally on the Company's intranet and externally at <https://www.google.com/policies/technologies/>. According to this webpage, these Principles guide decisions throughout Google in the Company's effort to balance innovation with the "appropriate level of privacy and security" for users.

EXTERNAL PRIVACY POLICY

Google also describes its privacy practices publicly through a primary privacy policy, available at <https://www.google.com/policies/privacy/>. According to this webpage, Google's external privacy policy is meant to help users understand, among other things, the data Google collects, why Google collects it, what Google does with it, and how Google protects it. Google's privacy policy is separated into the following main topics:

- Information collected;
- How information is used;
- Transparency and choice;
- Information shared by the user;
- How users can access and update personal information;
- User information Google shares;
- Information security;
- What products the privacy policy applies to;
- Regulatory compliance;
- Changes to the policy;
- Specific product practices; and
- Other useful privacy and security related materials.

Google maintains supplemental reference materials on the Company's external privacy policy webpage, most of which are embedded links throughout the policy, to provide additional clarification or information on a specific topic area of the policy. The webpage also contains links to archived versions of the policy. Each archived version includes a clean copy as well as a comparison showing marked changes from the previous version.

The Company provides additional information to users about its privacy practices on its Privacy & Terms website, including webpages on specific technologies and the Google Product Privacy Guide, available at <https://www.google.com/policies/>, on its Answers to Privacy and Security Questions site, available at <https://privacy.google.com>, and in various product Help Centers.

PRIVACY CONTROLS

The Google Privacy Program consists of internal and external tools, systems, processes, and other controls that Google has developed and implemented to protect user privacy. We describe these controls further in sub-section E. "Controls and Procedures" below.

C. Roles and Responsibilities

In this sub-section, we describe Google's privacy controls relating to Management Assertion 2: "Google has designated specific employees as officials responsible for the Google Privacy Program."

PRIVACY PROGRAM OWNERSHIP

Google's cross-functional Privacy and Security organization (PriSec) and affiliated PriSec teams are responsible for implementing and overseeing the Company's Privacy Program. The Privacy Program is led by the Director of Privacy for PriSec and the Director of Privacy Legal (privacy leadership). These individuals coordinate and oversee the Google Privacy Program, meeting regularly to discuss the Privacy Program. They have responsibility for:

- Periodically reviewing the Privacy Program for appropriateness and recommending adjustments, as deemed necessary;
- Instituting policies and procedures to promote compliance with global privacy laws and regulations;
- Ensuring that Privacy Program controls are implemented and effective;
- Reviewing and approving Privacy Risk Assessment results, which include the identification of opportunities to further reduce or mitigate risk;
- Reviewing, confirming, and submitting self-certifications to attest that Google products meet Safe Harbor requirements;
- Reviewing findings and recommendations that come as a result of testing of the Google Privacy Program; and
- Ensuring that action items identified from the results of control testing of the Google Privacy Program are assigned an owner and remediated.

ROLES, RESPONSIBILITIES, AND COMMUNICATION MODEL

PriSec's intranet website is available to all Google employees and identifies PriSec responsibilities, structure, teams, and other relevant information. The PriSec website contains webpages that provide a list and brief overview of each team within PriSec. Google employees can drill down into individual teams within PriSec through individual team pages, which provide a more granular-level description of the individual team, its function, and members, including contact information for each member. In this way, the website serves as a privacy organizational chart and communication model. PriSec consists of specialized and affiliated sub-teams that help engineers build privacy and security into Google products. PriSec-affiliated teams, including Privacy Legal, help support PriSec but do not report to PriSec leadership.

THE PRIVACY WORKING GROUP

The Privacy Working Group (PWG) is a specialized sub-team within PriSec that provides technical privacy expertise for different product areas (PAs) across Google. The PWG is comprised of more than a dozen smaller groups (also referred to as PWGs) that specialize in certain PAs. PWG team members include employees in various roles, including engineers (software, privacy, and security), program and product managers, and engineering managers. Generally, PWG acts as privacy consultants for the PAs. Some PAs have their own embedded PWG product teams, and other PAs have PWGs led by central privacy team members. PWG primarily provides oversight of the privacy review process for product launches. The team also provides engineering support for privacy-related products, guidance for privacy software-related improvements, and assistance performing privacy code audits. On an

ongoing basis, PWG meets to discuss privacy-related issues such as privacy launch reviews, new privacy risks, changes in Google's business operations, and privacy concerns raised by employees and users.

Based on our observations, summarized above, we conclude that Google's privacy controls and procedures satisfied the following Part III Order requirement:

A. The designation of an employee or employees to coordinate and be responsible for the privacy program.

D. Privacy Risk Assessment

In this sub-section, we describe Google's privacy controls relating to Management Assertion 3: "Google has implemented a privacy risk assessment process in order to identify reasonably foreseeable, material risks, both internal and external, as well as key privacy controls within processes including training, product design, development, and research that help to mitigate these risks."

RISK ASSESSMENT SCOPE

Google conducts annual privacy risk assessments to identify "reasonably foreseeable, material privacy risks, both internal and external," and to assess the Company's key privacy controls used to mitigate those risks. During the Reporting Period, a dedicated privacy risk assessment team conducted two privacy risk assessments. Team members for the privacy risk assessments included representatives from Privacy Legal, Engineering Compliance, Internal Audit, and the internal Google team responsible for managing the biennial assessment required under the Order.

During a privacy risk assessment, the team reviews documents and interviews privacy stakeholders across Google, including the PWG and employees from different PAs. (b)(3):6(f),(b)(4)

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

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

Based on our observations, summarized above, we conclude that Google's privacy controls and procedures satisfied the following Part III Order requirement:

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.

RISK ASSESSMENT RESULTS

At the end of each privacy risk assessment, Google's privacy risk assessment team identifies risk areas that may warrant additional mitigation, suggests additional or alternative privacy controls to improve the risk posture of covered information, and escalates these control recommendations as appropriate for evaluation and implementation. The team presents the results to privacy leadership, who review and must approve the final results. Thereafter, the team tracks risk assessment recommendations and Google's efforts to address them.

Based on our observations, summarized above, we conclude that Google's privacy controls and procedures satisfied the following Part III Order requirement:

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.

E. Controls and Procedures

In this sub-section, we describe Google's privacy controls relating to Management Assertion 4: "On an ongoing basis, Google implements reasonable privacy controls and procedures to address identified privacy risks."

PRIVACY LAUNCH REVIEW

The PWG reviews every Google product launch – for both new products and changes to existing products – to identify and communicate potential privacy concerns to the PA responsible for the launch. The PA is required to complete a Privacy Design Document (PDD), which contains a structured and consistent set of questions about the product's data lifecycle, covering data collection, use, notice/control, sharing, storage/access, and deletion/retention. In the case of a minor change to a product or incremental launch that is related to a main launch, the PA completes a Privacy Launch Document (PLD). The PLD contains a set of structured questions similar to the questions on the PDD, but the PLD's questions are intended to capture the data processing activities that may have changed since creation of the original PDD.

The PWG member assigned to the product launch must indicate approval of the privacy documentation (PDD or PLD) in Google's dedicated product launch tracking system prior to product launch. The PWG member communicates any privacy concerns to the PA, ensuring that these concerns are addressed before providing final approval. For some launches, the PWG member may request that a Privacy Code Audit (PCA) be performed. A PCA is a detailed, targeted review of a product's underlying code by Google software engineers to answer specific questions about the product's privacy controls and impacts. PWG members receive training and use their experience to determine when a PCA may be useful. (b)(3):6(f),(b)(4)

(b)

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

The code auditor creates a record of any issues observed during the PCA. After PWG prioritizes and remediates those issues, the PCA team issues the final report to all stakeholders. The PWG member will not approve the launch until the product team has remediates any launch-blocking findings.

END-USER PRIVACY SETTINGS AND TOOLS

Google provides privacy settings, guides, and tools for users to control how the Company collects, uses, and protects their data. We describe these controls briefly below.

TYPE	NAME	DESCRIPTION
Account Management Tools	My Account	Serves as the central hub of security, privacy, and general account settings, tools, and guides for each user
	Dashboard	Provides an "at-a-glance" view of the user's recent activity (e.g., how many documents and emails the user has saved) and lets the user manage product settings directly
	Activity Controls	Displays settings to manage, edit, and delete activity and data use associated with a user's account, including the user's searches and browsing activity
	Account Permissions for Connected Apps	Shows the applications and external websites connected to a user's Google account and allows the user to manage those permissions and remove applications as desired
	Inactive Account Manager	Allows the user to choose what happens to account data if an account becomes inactive for a length of time that the user specifies, including deleting the account or nominating a trusted contact who may access the account data when the account becomes inactive
	Account and Service Deletion	Allows the user to delete certain Google products (e.g., Gmail, Google+, etc.) or delete the user's entire Google account
Product Settings	Ads Settings	Allows the user to control the types of ads received by adjusting the user's interests and demographic details, and removing unwanted ads, or to opt-out of personalized ads altogether
	Google+/Social Settings	Allows the user to manage who can comment on the user's posts, see photos and videos the user shares on Google+, and view other details on the user's profile
	Search Settings	Allows the user to control search settings such as the use of SafeSearch filters and whether private results are included in their search results
	Analytics Opt-Out	Allows the user to control whether the user's data will be used by Google Analytics

TYPE	NAME	DESCRIPTION
Privacy Tools and Guides	Privacy Checkup	Facilitates a walkthrough of a user's products and services that allows the user to adjust privacy settings
	Product Privacy Guide	Contains links to articles with information about how Google's products work and how a user can manage their data within products
	Incognito Mode	Allows use of Google's Chrome browser without Chrome saving the pages viewed in Incognito windows
Security Tools and Guides	Security Checkup	Facilitates a walkthrough of a user's products and services that allows the user to adjust security settings, including the user's recovery information, recent security events, connected devices, and account permissions
	2-Step Verification	Allows the user to enable a stronger security sign-on process for the user's Google accounts that requires two forms of authentication (e.g., password and verification code)
	Device Activity and Notifications	Allows the user to review which devices have accessed the user's accounts and control how to receive alerts if Google detects potentially suspicious activity
	Service Encryption	Provides information about service encryption, which is available for several Google products, including Search, Maps, YouTube, and Gmail
	Chrome Safe Browsing	Provides warning messages about websites that could contain malware, unwanted software, and phishing schemes designed to steal personal information
Data Export	Download your data ³	Allows the user to download and export data from the user's Google accounts

Google also publishes and maintains an online "Transparency Report" that provides various reports to users, including information about government requests for information about users, copyright removal requests, product traffic, safe browsing, and "Right to Be Forgotten" claims. According to Google, the Transparency Report is intended to empower users to understand how laws and policies affect Internet users and the flow of information online, including the average volumes of various information requests and removal requests. Google's Transparency Report is available at www.google.com/transparencyreport.

³ Google renamed this tool, formerly known as "Takeout," during the Reporting Period.

PRIVACY TRAINING

Google requires new employees to take foundational privacy training upon employment and at least biennially thereafter. The course contains both standard content applicable to all employees and tailored content specific to an employee's role at Google (e.g., Sales, Marketing, Engineering). The training features real-world situations that require employees to select the correct privacy action for each scenario.

The PrivacyEDU team is responsible for creating, evaluating, and tracking mandatory and supplemental privacy training at Google. Their responsibilities with regard to the mandatory training include:

- Tracking compliance for all Google employees;
- Conducting ongoing "needs analysis," including quarterly meetings with relevant stakeholders to determine what kinds of privacy behaviors, skills, and knowledge they want Google employees to have, and how best to train them to achieve those goals;
- Analyzing training effectiveness; and
- Tracking behaviors to determine whether employees act in accordance with training content.

New engineers (external hires or internal transfers) are required to complete a separate training course focused on privacy considerations relevant to product design and user interface/user experience issues. The course includes information about Google's Privacy Principles and aims to make the principles actionable for engineering roles.

For both training courses, the PrivacyEDU team tracks user completion and sends automatic reminder emails to the employee to complete the training. After the internal training due date has passed, the employee's manager is copied on the reminder emails sent to the employee.

Google provides several opportunities for additional, ongoing privacy education. Each year, Google holds a "Privacy Week" that includes workshops, seminars, speeches, contests, and promotional items (e.g., posters, t-shirts, stickers) to support Privacy awareness across the Company. The Company also offers supplemental training courses by video or on the intranet, which Google employees can access at any time. These courses include:

- Intermediate topics (supplementary training focused on specific privacy topics, such as privacy for mobile devices);
- Advanced topics (supplementary technical privacy training intended primarily for engineers, TLs, and PMs);
- Professional training (intended primarily for those seeking the Certified International Privacy Professional designation); and
- Targeted training (privacy and security training designed especially for specific teams or individuals, available by request from a PM or other team lead).

INTERNAL AND EXTERNAL FEEDBACK PROCESSES

Google has established feedback processes providing internal users with the ability to voice privacy concerns. Feedback is monitored by the Google Privacy Team⁴ on a continuous basis. The principal method for Google employees to submit privacy-related feedback or questions is through an internal email address, which aggregates all feedback into a common "inbox" for PWG review. There is a weekly rotation of PWG members who are responsible for checking the inbox and responding to emails. The PWG member may answer questions or feedback directly but often refers (forwards) the email to the appropriate party for resolution.

Google has also established processes to collect privacy-related feedback from external users. Google collects external feedback through a variety of channels, some of which are product or location specific. Typical forms of feedback received include:

- Complaints, which may include product-specific privacy concerns, a user's improper use of another individual's personal information, or impersonation claims;
- Subject access requests, from users requesting to view or access their personal data that Google holds; and
- Content removals, for content that users deem offensive, illegal, or infringing of their privacy rights.

ADDITIONAL CONTROLS

Google's additional key privacy controls and procedures include:

- An incident response program for responding to privacy incidents;
- A U.S.-E.U. Safe Harbor Framework Program (Safe Harbor Program) in which Product Counsels, PMs, and TLs attest to the accuracy and comprehensiveness of the Privacy Program and the Safe Harbor Principles;⁵
- An entity-wide security program that supports the Privacy Program and is subject to external assessments;
- Mandatory confirmation of adherence to the Google Code of Conduct and confidentiality agreements upon employment; and
- Maintenance of a publicly available website linking to Google's privacy policy and other privacy resources.

⁴ "Privacy Team" is the term Google often uses to refer to privacy stakeholders, which include employees of the Privacy Legal, Privacy Working Group, and Privacy Engineering teams, among others.

⁵ As a result of the European Court of Justice's October 2015 decision invalidating Safe Harbor for data transfers from the European Union, Google is monitoring regulatory developments and preparing for changes in required activities and certifications. Review of this transition to comply with any new regulatory requirements is outside the scope of this Assessment.

We provide a complete listing of Google's key privacy controls and procedures, including our Assessment activities for each, in section VI of this Report.

Based on our observations, summarized above, we conclude that Google's privacy controls and procedures satisfied the following Part III Order requirement (emphasis added):

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.

See sub-section "F. Monitoring and Testing" below for Google's satisfaction of the second half of the Part III requirement.

F. Monitoring and Testing

In this sub-section, we describe Google's privacy controls relating to Management Assertion 5: "Google regularly tests or monitors the effectiveness of the privacy controls."

ONGOING MONITORING OF PRIVACY CONTROLS

Google's Internal Audit team (Internal Audit) regularly tests and monitors the effectiveness of the Company's privacy controls and procedures. During the initial scope-planning audit phase, Internal Audit considers whether and to what extent privacy should be included in the audit scope. Internal Audit team members who specialize in privacy and security meet with the party requesting the audit and product counsel or privacy counsel, as needed, to discuss the audit scope. If the audit is deemed privacy-relevant, Internal Audit develops privacy related audit steps based on the product(s) involved and audit scope. Google's Director of Internal Audit must approve all scoping decisions.

BIENNIAL PRIVACY PROGRAM ASSESSMENTS

Internal Audit also performs biennial audits of the Google Privacy Program controls that support the Assertions, when no external independent assessment is required under the Order. These audits are conducted separate from the annual privacy risk assessments discussed above. Internal Audit generally adopts the same methodology that the independent assessor uses for the external, independent assessments: Internal Audit gathers information using stakeholder interviews and document review and tests all of the same controls. Internal Audit may also test additional privacy areas and controls beyond those required under the Order.

The Internal Audit team provides stakeholders with bi-weekly status updates on audit progress and any potential areas of concern. Internal Audit communicates audit results to the Google Privacy Team, PWG stakeholders, and privacy leadership on a real-time basis.

SAFE HARBOR CERTIFICATION

The Company also maintains an internal Safe Harbor Program that provides the basis for Google's annual self-certification to the Department of Commerce to demonstrate compliance with the U.S.-E.U. Safe Harbor Framework. The Safe Harbor Program requires Product Counsels and PMs and/or TLs to internally certify product compliance with the Safe Harbor Principles. During the Reporting Period, Google completed two Safe Harbor self-certifications, each covering hundreds of products and features.

Product Counsels work with product engineers and PMs and/or TLs to ensure that all in-scope products are Safe Harbor compliant. Privacy Legal provides ongoing support to Product Counsels throughout the process as needed. In preparation for the Safe Harbor product review process, Privacy Legal annually prepares various internal Safe Harbor awareness and training resources, including internal websites and training for certification stakeholders. Privacy Legal also prepares various reference documents and guidance, such as:

- *Safe Harbor Legal Guide* – Provides an overview of the underlying Safe Harbor Principles and legal requirements;
- *Safe Harbor Process Guide* – Provides guidance on the operation of Google's Safe Harbor product review process, which provides a basis for Google's annual certification of compliance with the Safe Harbor Framework; and
- *Safe Harbor Product Counsel Checklist* – Details product requirements for complying with Safe Harbor Principles. The checklist describes the Safe Harbor Principles and steps required to achieve compliance with the Principles.

Based on our observations, summarized above, we conclude that Google's privacy controls and procedures satisfied the following Part III Order requirement (emphasis added):

*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.***

See sub-section "E. Controls and Procedures" above for Google's satisfaction of the first half of the Part III requirement.

G. Service Provider Oversight

In this sub-section, we describe Google's privacy controls relating to Management Assertion 6: "Google has developed and implemented reasonable steps to select and contract with service providers capable of appropriately protecting and maintaining the privacy of covered information received from Google."

PURCHASE REQUISITION REVIEW

Google has instituted processes to provide additional review and control for those service providers that will have access to user data. Google has developed and implemented a system to facilitate the review of purchase requisitions. Within this system, Google employees indicate whether a requisition will involve user data, which influences the type of review and privacy controls required. The Google Ethics & Compliance team (E&C) reviews requisitions where the service provider will have access to Google user data. E&C has controls in place to determine whether Google employees properly designate whether the engagement involves the personally identifiable information (PII) of Google users or employees (b)(3):6(f),(b)(4)

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

VENDOR SECURITY AUDITS

E&C refers purchase requisitions to the Vendor Security Team for a risk-based Vendor Security Audit (VSA) for what are internally described as "higher risk" requisitions (b)(3):6(f),(b)(4)

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

Any exceptions to the VSA process must be approved by a senior manager in Google's Security team in accordance with a documented Exception Approval Escalation Process.

Google service providers are also required to sign data protection and confidentiality terms as part of their contractual agreements. E&C specifies the terms to be included in the service provider contract based on the level of data access that the service provider will have. We believe that the terms included in these contracts provide for comprehensive confidentiality and data security protection. Google stakeholders attested that Internal Audit also considers and documents privacy-related risks in the scoping and execution of audits performed on Google's service providers.

Based on our observations, summarized above, we conclude that Google's privacy controls and procedures satisfied the following Part III Order requirement:

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.

H. Program Evaluation and Adjustment

In this sub-section, we describe Google's privacy controls relating to Management Assertion 7: "The Google Privacy Program is regularly evaluated and adjusted over time in light of the results of testing and monitoring, any material changes to Google's operations or business arrangements, or any other circumstances that Google knows may have a material impact on the effectiveness of the Google Privacy Program." Our description is brief, as we have described these program evaluation and adjustment processes more fully in the sub-sections above.

Google conducts ongoing privacy risk assessment processes as discussed above. Internal Audit also performs a periodic assessment of key Google privacy controls. Internal Audit results are communicated to relevant audit stakeholders on an ongoing basis and are presented to privacy leadership at audit conclusion. The internal Google team responsible for managing the Assessment required under the Order maintains a comprehensive list of all audit action items, assigns owners, and tracks the items to remediation. On a regular basis, the team also apprises privacy leadership about remediation progress.

Based on our observations, summarized above, we conclude that Google's privacy controls and procedures satisfied the following Part III Order requirement:

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.

Based on our observations, summarized in each sub-section above, we conclude that Google's privacy controls relating to roles and responsibilities for the Privacy Program are appropriate to Google's size and complexity, the nature and scope of Google's activities, and the sensitivity of the covered information.

VI. The Google Privacy Program: Assertions, Controls, Assessment Activities, and Assessment Results

In the table below, we list the Google Privacy Program Assertions and corresponding privacy controls, the Assessment activities performed by Promontory, and the Assessment results. We did not observe any exceptions to Google's Assertions or controls.

CONTROL	PROMONTORY ASSESSMENT ACTIVITIES PERFORMED	ASSESSMENT RESULTS
Assertion 1. Google has implemented and maintains a comprehensive privacy program, which is documented in written policies and procedures.		
1.1. The Google Privacy Program is documented in written policies.	(b)(3):6(f),(b)(4)	No exceptions noted

CONTROL	PROMONTORY ASSESSMENT ACTIVITIES PERFORMED	ASSESSMENT RESULTS
1.2. The Google Privacy Program is periodically reviewed for appropriateness.	(b)(3):6(f),(b)(4)	No exceptions noted
1.3. Internal Google privacy policies are periodically reviewed and updated as necessary.		No exceptions noted
Assertion 2. Google has designated specific employees as officials responsible for the Google Privacy Program.		
2.1. Privacy roles and responsibilities of employees and groups that play a part in privacy at Google are defined and published.	(b)(3):6(f),(b)(4)	No exceptions noted
2.2. Google maintains an online privacy organizational chart and communication model.		No exceptions noted

CONTROL	PROMONTORY ASSESSMENT ACTIVITIES PERFORMED	ASSESSMENT RESULTS
2.3. A working group of privacy subject matter experts provides oversight of privacy topics at Google.	(b)(3):6(f),(b)(4)	No exceptions noted
Assertion 3. On an ongoing basis, Google implements reasonable privacy controls and procedures to address identified privacy risks.		
3.1 (7.1). ⁶ The Google Privacy Team conducts periodic risk assessments to: <ul style="list-style-type: none"> • Identify external and internal risks; • Assess existing privacy controls; • Assess risks in product design, development, and research; • Consider changes in the regulatory environment; and • Consider the impact of any changes to Google operations or business arrangements (e.g., acquisitions, divestitures). 	(b)(3):6(f),(b)(4)	No exceptions noted

⁶ Where controls are the same, we cross-reference the control number using parentheses.

CONTROL	PROMONTORY ASSESSMENT ACTIVITIES PERFORMED	ASSESSMENT RESULTS
3.2 (7.2). The Google Privacy Team reviews the Risk Assessment results, and identifies opportunities to further reduce or mitigate risk.	(b)(3):6(f),(b)(4)	No exceptions noted
3.3. Risk Assessment results are communicated to Google management in a timely manner.		No exceptions noted
Assertion 4. Google has implemented a privacy risk assessment process in order to identify reasonably foreseeable, material risks, both internal and external, as well as key privacy controls within processes including training, product design, development, and research that help to mitigate these risks.		
4.1. Google's privacy design documentation is required to be completed, and privacy design is reviewed prior to product launch.	(b)(3):6(f),(b)(4)	No exceptions noted

CONTROL	PROMONTORY ASSESSMENT ACTIVITIES PERFORMED	ASSESSMENT RESULTS
<p>4.2. Google facilitates transparency and choice by providing end-user privacy settings which include:</p> <ul style="list-style-type: none"> Account management tools (e.g., My Account, Dashboard, Activity Controls, Account Permissions for Connected Apps and Sites, Inactive Account Manager, Account and Service Deletion); Product settings (e.g., Ads Settings, Google+/Social Settings, Search Settings, Analytics Opt-Out); Privacy tools and guides (e.g., Privacy Checkup, Product Privacy Guide, Incognito Mode); Security tools and guides (e.g., Security Checkup, 2-Step Verification, Device Activity and Notifications, Service Encryption, Chrome Safe Browsing); Tools for exporting user data from Google products (e.g., Download your data); and Google Transparency Report. 	<p>(b)(3):6(f),(b)(4)</p>	<p>No exceptions noted</p>

CONTROL	PROMONTORY ASSESSMENT ACTIVITIES PERFORMED	ASSESSMENT RESULTS
4.3. Google Privacy engineers perform privacy code audits, and results are reviewed by stakeholders.	(b)(3):6(f),(b)(4)	No exceptions noted
4.4. The Google Privacy Team provides supplemental training and awareness programs including a privacy awareness week, privacy workshops, and advanced privacy training courses.		No exceptions noted

CONTROL	PROMONTORY ASSESSMENT ACTIVITIES PERFORMED	ASSESSMENT RESULTS
<p>4.5. Google employees are required to complete training about Google privacy policies and practices within 90 days of hire date and at least biennially thereafter, and completion is followed-up on by management.</p>	<p>(b)(3):6(f),(b)(4)</p>	<p>No exceptions noted</p>
<p>4.6. Foundational privacy training is required of new Google engineers, and completion is followed-up on by management.</p>		<p>No exceptions noted</p>
<p>4.7. Google has established feedback processes that give internal users the ability to voice privacy concerns that are monitored by the Google Privacy Team.</p>		<p>No exceptions noted</p>

CONTROL	PROMONTORY ASSESSMENT ACTIVITIES PERFORMED	ASSESSMENT RESULTS
<p>4.8. Google has established feedback processes that give external users the ability to voice privacy concerns, which are monitored.</p>	<p>(b)(3):6(f),(b)(4)</p>	<p>No exceptions noted</p>
<p>4.9. Google has an incident response program in place with established processes for responding to privacy incidents. The program and its processes are documented and reviewed periodically. Privacy incidents are monitored and tracked in accordance with internal policy.</p>		<p>No exceptions noted.</p>

CONTROL	PROMONTORY ASSESSMENT ACTIVITIES PERFORMED	ASSESSMENT RESULTS
<p>4.10. On an annual basis, Google product managers and tech leads attest to the accuracy, comprehensiveness, and implementation of the Google Privacy Policy or that they have identified any changes that need to be made to reflect current practices.</p>	<p>(b)(3):6(f),(b)(4)</p>	<p>No exceptions noted</p>
<p>4.11. Google has an entity-wide information security program that supports the Google Privacy Program. Google engages third parties throughout the year to perform assessments of its security program.</p>		<p>No exceptions noted</p>

CONTROL	PROMONTORY ASSESSMENT ACTIVITIES PERFORMED	ASSESSMENT RESULTS
4.12. Google employees are required to sign a Code of Conduct acknowledgement upon employment.	(b)(3):6(f),(b)(4)	No exceptions noted
4.13. Google employees are required to sign confidentiality agreements upon employment.		No exceptions noted
4.14. Google maintains a site containing its privacy policy and supplemental reference materials explaining its policy at www.google.com/policies/privacy .		No exceptions noted

CONTROL	PROMONTORY ASSESSMENT ACTIVITIES PERFORMED	ASSESSMENT RESULTS
Assertion 5. Google regularly tests or monitors the effectiveness of the privacy controls.		
5.1. Privacy is considered and documented as part of scoping and execution (where applicable) for internal audits at Google.	(b)(3):6(f),(b)(4)	No exceptions noted

CONTROL	PROMONTORY ASSESSMENT ACTIVITIES PERFORMED	ASSESSMENT RESULTS
<p>5.2 (7.3). Internal Audit performs a periodic assessment of key Google privacy controls. Results are shared with the Google Privacy Team and other stakeholders as necessary and are considered for ongoing improvement of the privacy program.</p>	<p>(b)(3):6(f),(b)(4)</p>	<p>No exceptions noted</p>
<p>5.3. Google management periodically reviews internal reports on the functioning of the privacy review process.</p>		<p>No exceptions noted</p>

CONTROL	PROMONTORY ASSESSMENT ACTIVITIES PERFORMED	ASSESSMENT RESULTS
5.4. Google management reviews and confirms the completion of the Safe Harbor process for Google.	(b)(3):6(f),(b)(4)	No exceptions noted
Assertion 6. Google has developed and implemented reasonable steps to select and contract with service providers capable of appropriately protecting and maintaining the privacy of covered information received from Google.		
6.1. The Google Ethics & Compliance team reviews purchase requisitions and refers service providers to the Vendor Security Audit team based on risk.	(b)(3):6(f),(b)(4)	No exceptions noted

CONTROL	PROMONTORY ASSESSMENT ACTIVITIES PERFORMED	ASSESSMENT RESULTS
6.2. Google service providers are required to sign confidentiality terms as part of the agreement, as deemed necessary.	(b)(3):6(f),(b)(4)	No exceptions noted
6.3. Google teams review Google service providers using a risk-based assessment process.		No exceptions noted

CONTROL	PROMONTORY ASSESSMENT ACTIVITIES PERFORMED	ASSESSMENT RESULTS
Assertion 7. The Google Privacy Program is regularly evaluated and adjusted over time in light of the results of testing and monitoring, any material changes to Google's operations or business arrangements, or any other circumstances that Google knows may have a material impact on the effectiveness of the Google Privacy Program.		
<p>7.1 (3.1). The Google Privacy Team conducts periodic risk assessments to:</p> <ul style="list-style-type: none"> Identify external and internal risks; Assess existing privacy controls; Assess risks in product design, development, and research; Consider changes in the regulatory environment; and Consider the impact of any changes to Google operations or business arrangements (e.g., acquisitions, divestitures). 	(b)(3):6(f),(b)(4)	No exceptions noted
<p>7.2 (3.2). The Google Privacy Team reviews the Risk Assessment results, and identifies opportunities to further reduce or mitigate risk.</p>		No exceptions noted

CONTROL	PROMONTORY ASSESSMENT ACTIVITIES PERFORMED	ASSESSMENT RESULTS
7.3 (5.2). Internal Audit performs a periodic assessment of key Google privacy controls. Results are shared with the Google Privacy Team and other stakeholders as necessary and are considered for ongoing improvement of the privacy program.	(b)(3):6(f),(b)(4)	No exceptions noted
7.4. Findings and recommendations that come as a result of testing of the Google Privacy Program are communicated to privacy leadership as applicable. ⁷		No exceptions noted

⁷ Initial conversations with Google indicated that the Google Privacy team intends for controls 7.4 and 7.5 to speak to Internal Audit testing alone. Therefore, our review activities for controls 7.4 and 7.5 covered only Internal Audit findings, recommendations, and action items.

CONTROL	PROMONTORY ASSESSMENT ACTIVITIES PERFORMED	ASSESSMENT RESULTS
7.5. Action items identified from the results of control testing of the Google Privacy Program are assigned an owner and tracked to ensure remediation.	(b)(3):6(f),(b)(4)	No exceptions noted

VII. Management's Assertion

The management of Google Inc. (Google or the Company) represents that as of and for the two years ended April 25, 2016 (the Reporting Period), in accordance with Parts III and IV of the Agreement Containing Consent Order File No: 1023136 (the Order), with a service date of October 28, 2011, between Google and the Federal Trade Commission (FTC), the Company established and implemented a comprehensive Privacy Program (the Google Privacy Program) based on Company-specific criteria (described in paragraph three of this assertion); the Company's privacy controls were operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information; and the privacy controls have so operated throughout the Reporting Period.

Furthermore, the Company represents that for the Reporting Period, the privacy controls within the Google Privacy Program as described on pages 25-41 are appropriate to its size and complexity, the nature and scope of its activities, and the sensitivity of the covered information.

The Company-specific criteria (management assertions) used as the basis for the Google Privacy Program are described below. The below management assertions have corresponding controls as described on pages 25-41.

Assertion #1: Google has implemented and maintains a comprehensive privacy program, which is documented in written policies and procedures.

Assertion #2: Google has designated specific employees as officials responsible for the Google Privacy Program.

Assertion #3: Google has implemented a privacy risk assessment process in order to identify reasonably foreseeable, material risks, both internal and external, as well as key privacy controls within processes including training, product design, development, and research that help to mitigate these risks.

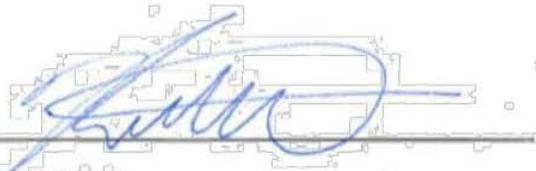
Assertion #4: On an ongoing basis, Google implements reasonable privacy controls and procedures to address identified privacy risks.

Assertion #5: Google regularly tests or monitors the effectiveness of the privacy controls.

Assertion #6: Google has developed and implemented reasonable steps to select and contract with service providers capable of appropriately protecting and maintaining the privacy of covered information received from Google.

Assertion #7: The Google Privacy Program is regularly evaluated and adjusted over time in light of the results of testing and monitoring, any material changes to Google's operations or business arrangements, or any other circumstances that Google knows may have a material impact on the effectiveness of the Google Privacy Program.

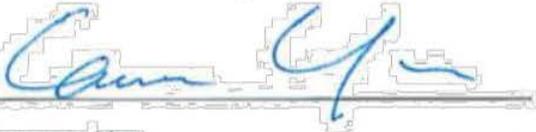
Google Inc.

By: 

Keith Enright

Director, Privacy Legal

Google Inc.

By: 

Lawrence You

Director of Privacy, Product and Engineering

Google Inc.

VIII. Appendix A – Assessment Interviews Summary

Promontory interviewed individuals in the following roles, who described and/or presented evidence to support the Assertions and corresponding privacy controls.

ROLE	TEAM
Compliance Analyst	Ethics & Compliance
Director, Privacy Legal	Legal
Director, Information Security	Privacy Incident Response
Director of Privacy	Privacy Engineering
IT Auditor - Security & Privacy	Internal Audit
Lead Privacy Program Manager	PrivacyEDU
Legal Specialist	Learning & Development
Legal Specialist	Legal
Privacy Counsel	Legal
Privacy Program Manager	Privacy Working Group
Privacy Program Manager	PrivacyEDU
Senior Counsel	Ethics & Compliance
Senior Manager	Engineering Compliance
Senior Manager	Internal Audit
Senior Privacy Counsel	Legal

IX. Appendix B – Google Teams Providing Evidence or Input

Promontory received evidence or input supporting the Google Assertions and corresponding privacy controls from the following teams:

- Compliance
- Engineering Compliance
- Ethics & Compliance
- Human Resources
- Information Security
- Internal Audit
- Learning & Development
- Legal
- Privacy Code Audit team
- Privacy Engineering
- Privacy Incident Response
- PrivacyEDU
- Product & Engineering
- The Privacy Working Group

X. Appendix C – Types of Evidence Reviewed

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



Promontory Financial Group, LLC
801 17th Street, NW, Suite 1100 | Washington, DC 20006
+1 202 384 1200 | promontory.com