



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

APR 03 2015

Chris Hoofnagle
UC Berkeley School of Law
344 Boalt Hall
Berkeley, CA 94720

Re: FOIA-2015-00729
Independent assessors report

Dear Mr. Hoofnagle:

This is in response to your request dated March 12, 2015, under the Freedom of Information Act seeking access to Google's privacy assessment for the years 2012-2014. In accordance with the FOIA and agency policy, we have searched our records as of March 12, 2015, the date we received your request in our FOIA office.

Your request did not indicate an agreement to pay any fees associated with the processing of your request. However, the Commission's fee regulations specify that fees less than \$25 will be waived. *See* 16 C.F.R. § 4.8(b)(4). Because the fees associated with the processing of your request did not exceed \$25, we have processed your request free of charge. In the future, please provide a fee agreement to facilitate the processing of your request.

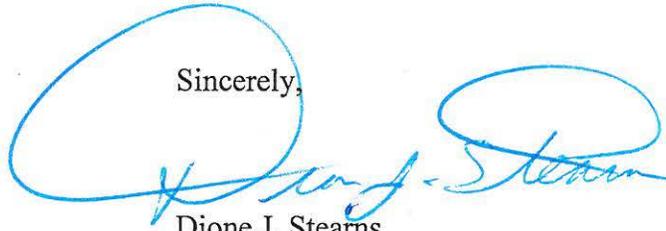
We have located 60 pages of responsive records. I am granting partial access to the accessible records. Portions of these pages fall within the exemptions to the FOIA's disclosure requirements, as explained below.

Portions of the responsive pages constitute confidential commercial or financial information, which is exempt from disclosure under FOIA Exemption 4, 5 U.S.C. § 552(b)(4). *See Critical Mass Energy Project v. NRC*, 975 F.2d 871, 879 (D.C. Cir. 1992). Moreover, because Section 6(f) of the FTC Act, 15 U.S.C. § 46(f), prohibits public disclosure of this type of information, it is also exempt under FOIA Exemption 3, 5 U.S.C. § 552(b)(3), which exempts from disclosure any information that is protected from disclosure under another federal statute.

If you are not satisfied with this response to your request, you may appeal by writing to Freedom of Information Act Appeal, Office of the General Counsel, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington D.C. 20580, within 30 days of the date of this letter. Please enclose a copy of your original request and a copy of this response. If you believe that we should choose to disclose additional materials beyond what the FOIA requires, please explain why this would be in the public interest.

If you have any questions about the way we handled your request or about the FOIA regulations or procedures, please contact Andrea Kelly at (202) 326-2836.

Sincerely,

A handwritten signature in blue ink, appearing to read "Dione J. Stearns". The signature is written in a cursive style with a large, looping initial "D".

Dione J. Stearns
Assistant General Counsel



Independent Assessor's Report on Google's Privacy Program

Biennial Assessment Report

For the period April 26, 2012 to April
25, 2014

The contents of this document, including the Report of Independent Accountants, contain PricewaterhouseCoopers LLP 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 document constitutes and reflects work performed or information obtained by PricewaterhouseCoopers LLP, in our capacity as independent assessor for Google Inc. for the purpose of Google Inc.'s Order. The document contains proprietary information, trade secrets and confidential commercial information of our firm and Google Inc. that is privileged and 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 FTC containing information derived from the report. We further request that written notice be given to PwC and Google Inc. before distribution of the information in the report (or copies thereof) to others, including other governmental agencies, to afford our firm and Google Inc. with 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 U.S. Federal Trade Commission and is not intended to be and should not be used by anyone other than these specified parties.

HIGHLY CONFIDENTIAL



Table of Contents

Table of Contents

Introduction 3

Report of Independent Accountants 4

Google’s Privacy Program Overview..... 6

PwC’s Privacy Assessment Approach 10

PwC’s Assessment of Part IV A, B, C, D of the Order15

**The Google Privacy Program: Assertions, Control Activities and PwC’s Tests
Performed and Results..... 20**

Appendix A – Assessment Interviews Summary 57



Introduction

Google Inc. (“Google” or the “Company”) and the Federal Trade Commission (“FTC”) entered into Agreement Containing Consent Order File No: 1023136 (the “Order”), which was served on October 28, 2011.

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.

Part IV of the Order requires Google 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. Google engaged PricewaterhouseCoopers LLP (“PwC” or “Assessor”) to perform this biennial assessment.

As described on pages 15-19, Google established its privacy program by implementing privacy controls to meet or exceed the protections required by Part III of the Order. As described on pages 11-14, PwC performed inquiry, observation, and inspection/examination procedures to assess the effectiveness of the Google privacy controls implemented to meet or exceed the protections required by Part III of the Order during the period April 26, 2012 through April 25, 2014, and our conclusions are on pages 4-5.

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



Report of Independent Accountants

To the Management of Google Inc.:

We have examined Management's Assertion, that as of and for the two years ended April 25, 2014, and throughout the period August 1, 2013 to April 25, 2014, as it relates to Motorola Mobility LLC's ("Motorola" or "MML") privacy controls (the "Assessment 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 Inc. ("Google" or the "Company") and the Federal Trade Commission ("FTC"), the Company had established and implemented a comprehensive Privacy Program, as described in Management's Assertion (the "Google Privacy Program"), based on Company specific criteria; and the privacy controls were operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the Assessment Period.

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

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and accordingly, included examining, on a test basis, evidence supporting the effectiveness of the Google 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 Google's interpretation of, or compliance with, information security or privacy-related laws, statutes, and regulations applicable to Google in the jurisdictions within which Google operates. We are also not responsible for Google's interpretation of, or compliance with, information security or privacy-related self-regulatory frameworks. Therefore, our examination did not extend to the evaluation of Google's interpretation of or compliance with information security or privacy-related laws, statutes, regulations, and privacy-related self-regulatory frameworks with which Google has committed to comply.

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

In our opinion, Google'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 Assessment Period, in all material respects as of and for the two years ended April 25, 2014, and throughout the period August 1, 2013 to April 25, 2014, as it relates to Motorola's privacy controls, based upon the Google Privacy Program set forth in Management's Assertion.



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

This report is intended solely for the information and use of the management of Google 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, California
June 23, 2014



Google's Privacy Program Overview

Company Overview

Google Inc. ("Google" or "the Company") was founded in 1998 by Larry Page and Sergey Brin. It began as a search engine. Since then, Google has grown to become a company offering a variety of services, including Gmail, Google Maps, Google Apps, Blogger, Chrome, Android, YouTube, and Google+, to users around the world.

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

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

Motorola is a mobile communications organization that invented many of the protocols and technologies that make mobile communications possible. Today, Motorola makes Android smartphones and Bluetooth accessories to keep people connected.

The following description of the Google Privacy Program and references throughout this report to the program and controls apply to both Google and Motorola, unless a distinction is otherwise noted.

Google Privacy Program Overview and Scope

The Google Privacy Program aims to ensure that Google's products and services consistently promote five core privacy principles (the "Privacy Principles"):

1. Use information to provide Google 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; and
5. Be a responsible steward of the information Google holds.

Google has developed a comprehensive privacy program, which is focused on carrying out the Company's commitment to protecting user privacy.

Google's commitment is reflected in the products and tools that it has built to keep users safe and give them choice and control. The Google Dashboard enables users to change their privacy settings for most Google products from one central location. Google provides all of its users with 2-step verification to protect their accounts from unauthorized access, among other tools. Users can also control the information they share with Google through various privacy controls. For example, Google+ Circles allows users to control what information they share and who can see it, so users can share content such as Google+ posts, YouTube videos or Local listings with the right people.



Privacy Program Governance and Accountability

The Google Privacy Program includes a cross-functional team from Privacy Engineering, Legal, Product & Engineering, Public Policy, and Communications. The various teams that support the Privacy Program collaborate to protect and improve the privacy of Google users, as well as work to promote compliance with the privacy related laws applicable to Google in the various jurisdictions within which Google operates.

Two central aspects of the Privacy Program are the privacy innovation and protection efforts of the Privacy Engineering Team, and the privacy legal compliance efforts of the Privacy Legal Team.

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

The Privacy Engineering Team works with other engineering and product teams to provide privacy support across the lifecycle of a product.

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

The Privacy Program also ensures the ongoing maintenance of privacy protections through continued work with product teams. For example, on an annual basis, Google product managers and tech leads work with lawyers to complete a comprehensive privacy review of their products as part of the US-EU and US-Swiss Safe Harbor programs. (b)(3):6(f), (b)(4)

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



In addition to the Privacy Engineering Team, Google's Legal Team serves as an important part of the Privacy Program. Google's Legal Team includes a number of attorneys designated as "Product Area Attorneys" who serve as the primary legal counsel for individual product teams. Product Area Attorneys are responsible for ensuring that products or services comply with relevant legal requirements, including those relating to privacy. In addition, Google's legal department includes a team of lawyers and staff (the "Privacy Legal Team") that provide legal support and advice to Product Area Attorneys as needed. The Privacy Legal Team is also responsible for supporting review of privacy design documentation to identify privacy legal concerns, and to provide legal guidance and support regarding privacy law to other Google teams and employees as appropriate.

While designated employees carry leadership responsibility for coordinating the Privacy Program across the Company, responsibility for privacy permeates most teams at Google. Many employees across teams and functions at Google are responsible for additional aspects of the Privacy Program, including Product & Engineering, Communications, and Public Policy.

Privacy Risk Assessment Process and Program Monitoring

In order to identify the privacy controls that are appropriate to Google's size and complexity, the nature and scope of Google's activities, and the sensitivity of the covered information as defined in the Order, Google has implemented a privacy risk assessment process. This process is focused on identifying reasonably foreseeable, material privacy risks, both internal and external, as well as key privacy controls, including training, product design, development, and research, that help to mitigate these risks. Refer to pages 20-54 below for a list of Google's privacy assertions and controls identified as a result of the privacy risk assessment.

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



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



PwC's Privacy Assessment Approach

PwC's Assessment Standards

Part IV 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 that 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

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

PwC Assessment Process Overview

The procedures performed by PwC were designed to:



- Assess the applicability of the safeguards selected by the Company to address the Company's obligations within the Order;
- Assess the design effectiveness of the safeguards implemented by the Company to address the relevant risks; and
- Assess the operating effectiveness of the implemented safeguards for the Assessment Period.

To evaluate Google's privacy risk assessment process and the design and implementation of controls to mitigate the risks identified from the privacy risk assessment, PwC designed and performed the following procedures.

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

In addition, PwC designed and performed procedures to evaluate the operating effectiveness of the control activities implemented by Google for the Assessment Period.

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

Refer below for a description of the test procedures utilized by PwC to assess the design and effectiveness of Google's privacy controls. Detailed test plans for each control tested are also included on pages 20-54 of this document.

Inquiry: To understand the design of the safeguards implemented and how they operate to meet or exceed the protections required by Part III of the Order (b)(3):6(f), (b)(4)

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



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



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

As described earlier in the report, the Google Privacy Program is based upon the management defined criteria, and is structured by assertions supported by controls to meet the stated assertions. (b)(3):6(f), (b)(4)

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



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

The tables in section "The Google Privacy Program: Assertions, Control Activities and PwC's Tests Performed and Results" of this report describe the scope of the Google Privacy Program referenced in the Management Assertion on pages 55-56. Google established its privacy program by implementing privacy controls to meet or exceed the protections required by Part III of the Order. The table also includes PwC's inquiry, observation, and inspection/examination test procedures to assess the effectiveness of the Google Privacy 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 20-54, Google has listed the privacy controls that were implemented and maintained during the Assessment Period. The table includes PwC's test procedures to assess the effectiveness of each safeguard as well as the results of such tests.

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.

As described in Google's Privacy Program Overview section above, based on the size and complexity of the organization, the nature and scope of Google's activities, and the sensitivity of the covered information (as defined by the Order), Google management developed the Company specific criteria (assertions) detailed on pages 20-54 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 Google's privacy risk assessment.

To evaluate Google's privacy risk assessment process and the design and implementation of controls to mitigate the risks identified from the risk assessment, PwC designed and performed the following procedures.

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



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

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

As summarized in the Google Privacy Program Overview on pages 6-9, Google has implemented the following protections to meet or exceed the protections required by Part III of the Order. The table on pages 20-54 includes the full list of Google's privacy controls, which have been implemented and maintained by Google to meet or exceed the protections required by Part III of the Order. The following paragraphs describe how the controls meet or exceed the protections required by Part III of the Order:

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

As described above, Google has designated a team of employees to coordinate and be responsible for the privacy program as required by Part III of the Order. As described on pages 10-14, PwC performed test procedures to assess the effectiveness of the Google privacy controls implemented to meet or exceed the protections required by Part III of the Order.

The Google Privacy Program includes a cross-functional team from Privacy Engineering, Legal, Product & Engineering, Public Policy, and Communications. The various teams that support the Privacy Program collaborate to protect and improve the privacy of Google users, as well as work to promote compliance with the privacy related laws applicable to Google in the various jurisdictions within which Google operates.

Two central aspects of the privacy program are the privacy innovation and protection efforts of the Privacy Engineering team, and the privacy legal compliance efforts of the Privacy Legal Team.

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

In addition to the Privacy Engineering Team, Google's Legal Team serves as an important part of the privacy program. Google's Legal Team includes a number of attorneys designated as "Product Area Attorneys" who serve as the primary legal counsel for individual product teams. Product Area Attorneys are responsible for ensuring that products or services comply with relevant legal requirements, including those relating to privacy. In addition, Google's legal department includes a team of lawyers and staff (the "Privacy Legal Team") that provide legal support and



advice to Product Area Attorneys as needed. The Privacy Legal Team is also responsible for supporting review of privacy design documentation to identify privacy legal concerns, and to provide legal guidance and support regarding privacy law to other Google teams and employees as appropriate.

While designated employees carry leadership responsibility for coordinating the privacy program across the Company, responsibility for privacy permeates most teams at Google. Many employees across teams and functions at Google are responsible for additional aspects of the Privacy Program, including Product & Engineering, Communications, and Public Policy.

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 in the Google Privacy Program description above, Google has identified reasonably foreseeable, material risks, both internal and external, that could result in Google'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 III of the Order. As described on pages 10-14, PwC performed test procedures to assess the effectiveness of the Google privacy controls implemented to meet or exceed the protections required by Part III of the Order.

In order to identify the privacy controls that are appropriate to Google's size and complexity, the nature and scope of Google's activities, and the sensitivity of the covered information as defined in the Order, Google has implemented a privacy risk assessment process. This process is focused on identifying reasonably foreseeable, material privacy risks, both internal and external, as well as key privacy controls, including training, product design, development, and research, that help to mitigate these risks. Refer to pages 20-54 below for a list of Google's privacy assertions and controls identified as a result of the privacy risk assessment.

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



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

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, Google 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 III of the Order.

Design & Implementation of Controls

Based on the risks identified through the risk assessment described in B. above, Google designed and implemented the privacy controls documented in the table on pages 20-54.

Regular Testing & Monitoring of Safeguards

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

The table on pages 20-54 also describes PwC's assessment of the controls the Company has identified and maintained to monitor the Google Privacy Program.

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.

Google has developed and implemented reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from Google as required by Part III of the Order. (b)(3):6(f),(b)(4)

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



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

As described on pages 20-54, PwC performed test procedures to assess the effectiveness of the Google privacy controls implemented to meet or exceed the protections required by Part III 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, as part of Google's ongoing privacy risk assessment processes, Google considers internal and external risks, existing privacy controls, risks in product design, development and research, changes in the regulatory environment, and the impact of any changes to Google's business operations or business arrangements.

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

As described on pages 11-14, PwC performed test procedures to assess the effectiveness of the Google privacy controls implemented to meet or exceed 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.

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



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

Provided below are the Google Privacy Program assertions, control activities, 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.

Test	Google Privacy Program Assertion	Control Activities	PwC's Tests Performed	PwC's Test Results
Assertion 1 –Google has implemented and maintains a comprehensive privacy program, which is documented in written policies and procedures.				
1.1-G	The Google Privacy Program is documented in written policies.	(b)(3):6(f),(b)(4)		
1.1-M	The MML privacy controls are documented in written policies	(b)(3):6(f),(b)(4)		



Key	Control Description	Control Objective	Control Design	Control Effectiveness
		(b)(3):6(f), (b)(4)		
1.2-G	The Google Privacy Program is periodically reviewed for appropriateness.			
1.2-M	The MML privacy controls are periodically reviewed for appropriateness.			



Key	Description of Finding	Business Impact	Risk Rating	Mitigation Strategy
		(b)(3):6(f),(b)(4)		
1.3-G	Internal Google privacy policies are periodically reviewed and updated as necessary.			
1.3-M	Internal MML privacy policies are periodically reviewed and updated as necessary.			



Index	Company Name or Website	Description of Organization	Data to be Disclosed	Data to be Redacted
Assertion 2 - Google has designated specific employees as officials responsible for the Google Privacy Program.				
2.1-G	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)		
2.1-M	Privacy roles and responsibilities of employees and groups that play a part in privacy at MML are defined and published.			
2.2-G	Google maintains an online privacy organizational chart and communication model.			
2.2-M	MML maintains an online privacy organizational chart and communication model.			



Identify	Specify the Issue	Assess the Exposure	Identify Controls	Additional Information
2.3-G	A working group of privacy subject matter experts, (b)(3):6(f), (b)(4) (b)(3): provides oversight of privacy topics at Google.	(b)(3):6(f), (b)(4)		
2.3-M	A working group of privacy subject matter experts, (b)(3):6(f) (b)(4) (b)(3): provides oversight of privacy topics at MML.			
Assertion 3 - Google has implemented internal and external, as well as key privacy help to mitigate these risks.				
3.1-G	The Google privacy team conducts periodic risk assessments to: <ul style="list-style-type: none">Identify external and internal risks;Assess existing privacy controls including privacy training to Googlers;			



Date	Description of the subject statement (with date)	Reference to management	Description of the subject	Confidentiality information
	<ul style="list-style-type: none">Assess risks in (b)(3) (b)(3):6(f),(b)(4)Consider changes in the regulatory environment; andConsider the impact of any changes to Google operations or business arrangements (e.g., acquisitions, divestitures).	(b)(3):6(f),(b)(4)		



Item	Compliance Review Details	Description of Deficiency	Risk Rating	Action Plan Implementation
		(b)(3):6(f),(b)(4)		
3.1-M	<p>The MML privacy team conducts periodic risk assessments to:</p> <ul style="list-style-type: none">• Identify external and internal risks;• Assess existing privacy controls including privacy training to new hires;• Assess risks in (b)(3):6(f),(b)(4)• Consider changes in the regulatory environment; and• Consider the impact of any changes to MML operations or business			



(b)(3)	Acquire, Dispose, or Sell	Risk Assessment	Mitigation	Additional Information
	arrangements (e.g., acquisitions, divestitures).	(b)(3):6(f),(b)(4)		
3.2-G	The Google privacy team reviews the Risk Assessment results, and identifies opportunities to further reduce or mitigate risk.			



Risk	Control Description	Risk Mitigation	Residual Risk	Additional Information
3.2-M	The MML privacy team reviews the Risk Assessment results, and identifies opportunities to further reduce or mitigate risk.	(b)(3):6(f),(b)(4)		
3.3-G	Risk Assessment results are communicated to Google management in a timely manner.			
3.3-M	Risk Assessment results are communicated to MML management in a timely manner.			
Assertion 4 - On an ongoing basis, Google implements reasonable privacy controls and procedures to address identified privacy risks.				
4.1-G	(b)(3):6(f),(b)(4)			



Risk	Strategic Impact	Relevance to Business	Legal, Reg. or Govt.	Additional Information
4.1-M	(b)(3):6(f), (b)(4)	(b)(3):6(f), (b)(4)		
4.2-G	Google facilitates transparency and choice by providing end-user privacy settings which include: <ul data-bbox="425 809 702 1230" style="list-style-type: none">• Dashboards (Account Dashboard, Transparency Report);• Security Tools (2-Step Verification, Recent Activity, Account Permissions, SSL);• Account Management and Social Settings;• Ad Settings;• Me on the Web;• Incognito Mode;• Inactivity Mode; and• Takeout.	(b)(3):6(f), (b)(4)		



Ref.	Findings and Remedial Actions	Risk Rating	Risk Mitigation	Significant Findings
4.2-M	<p>MML facilitates transparency & choice by providing end-user privacy settings on new products</p> <p>(b)(3):6(f), (b)(4)</p> <ul style="list-style-type: none">• Cookie control tool;• Global opt-out tool (outout.motorola.com) for marketing email; and• privacy@motorola.com.	(b)(3):6(f), (b)(4)		
4.3-G	<p>(b)(3):6(f), (b)(4)</p>			



ID	Description	Findings	Recommendations	Status
4.4-G	The Google Privacy Team provides periodic supplemental training and awareness programs (b)(3):6(f), (b)(4)	(b)(3):6(f), (b)(4)		
4.4-M	The MML Privacy Team provides periodic supplemental training and awareness programs (b)(3):6(f), (b)(4)			
4.5-G	Google employees are required to complete training that includes Google privacy policies and practices (b)(3):6 (b)(3):6(f), (b)(4)			



Item	Description of Findings	Impact/Significance	Cause/Contributing Factors	Additional Comments
		(b)(3):6(f),(b)(4)		
4.5-M	MML employees are required to complete training that includes MML privacy policies and practices (b)(3):6(f),(b)(4)	(b)(3):6(f),(b)(4)		



Page	Section Reference	Findings	Risk Rating	Control Effectiveness
		(b)(3):6(f),(b)(4)		
4.6-G	Foundational privacy training is required of new Google engineers (b)(3):6(f),(b)(4)			
4.7-G	(b)(3):6(f),(b)(4)			



Task	Description of activity	Status of activity	Date of completion	Project manager
4.7-M	(b)(3):6(f),(b)(4)			
4.8-G				
4.8-M				



Ref	Variable or Control State	Control Type / Intervention	Regulatory Source	Additional Information
	(b)(3):6(f),(b)(4)			
4.9-G				
4.9-M				



Mat.	Classification Agency	Type of Information	Reference Number	Additional Information
	(b)(3):6(f),(b)(4)			
4.10-G				
4.10-M				
4.11-G				



ID	Project Name	Project Description	Reporting Period	Status
	(b)(3):6(f),(b)(4)			
4.11-M				



Key	Sample Control Methods	Description of Method	Risk Rating	Additional Information
4.12-G	(b)(3);6(f),(b)(4)			
4.12-M				



No.	Description of Control	Frequency of Testing	Number of Controls	Additional Controls
		(b)(3):6(f),(b)(4)		
4.13-G	(b)(3):6(f),(b)(4)			
4.13-M				
4.14-G				



Date	Description of Activity	Amount (in thousands)	Account Number	Classification
		(b)(3):6(f),(b)(4)		
4.14-M	(b)(3):6(f),(b)(4)	(b)(3):6(f),(b)(4)		
4.15-G	(b)(3):6(f),(b)(4)			
4.15-M				



Risk	Control (or) Remedial Action	Risk (or) Control Deficiency	Materiality	Significance
	materials explaining its policies.	(b)(3):6(f),(b)(4)		
Assertion 5 - Google regularly tests or monitors the effectiveness of the privacy controls.				
5.1-G	(b)(3):6(f),(b)(4)			
5.1-M				



DOI	Contract Number	Contract Description	Contract Quantity	Contract Amount
	(b)(3):6(f),(b)(4)	(b)(3):6(f),(b)(4)		
5.2-G				
5.2-M				



ID	Classification	Sensitivity	Control	Approval
	(b)(3):6(f),(b)(4)			
5.3-G				
5.3-M				



Item	Description of Assertion	Control Description	Control Objective	Additional Information
		(b)(3):6(f),(b)(4)		
5.4-G	Management reviews and confirms the completion of the Safe Harbor process for Google.			
5.4-M	European Binding Corporate Rules (BCRs) are in place at MML as a trans-border dataflow compliance mechanism.			
Assertion 6 - Google has developed an appropriately protecting and maintaining				
6.1-G	(b)(3):6(f),(b)(4)			



Type	Category (if applicable)	Number of pages disclosed	Date of disclosure	Authorized information
		(b)(3):6(f),(b)(4)		
6.1-M	(b)(3):6(f),(b)(4)			
6.2-G				
6.2-M				



ID#	Report Name	Type	Status	Additional Information
	(b)(3):6(f),(b)(4)			
6.3-G				
6.3-M				



Risk	Privacy, Security, Controls	Risk, Impact, Remediation	Materiality, Frequency	Mitigation Strategy
6.4-G	(b)(3):6(f),(b)(4)			
6.4-M				
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.				
7.1-G	The Google privacy team conducts periodic risk assessments to: Identify external and	(b)(3):6(f),(b)(4)		



Topic	Strategic, Operational, or Policy	Key Strengths and Weaknesses	Critical Risks and Opportunities	Anticipated Mitigation/Response
	<p>internal risks;</p> <ul style="list-style-type: none">Assess existing privacy controls including privacy training to Googlers;Assess risks in (b)(3); (b)(3):6(f), (b)(4)Consider changes in the regulatory environment; andConsider the impact of any changes to Google operations or business arrangements (e.g., acquisitions, divestitures).		(b)(3):6(f), (b)(4)	



ID	Control Objective	Control Description	Control Frequency	Control Status
		(b)(3):6(f),(b)(4)		
7.1-M	<p>The MML privacy team conducts periodic risk assessments to:</p> <p>Identify external and internal risks;</p> <ul style="list-style-type: none">Assess existing privacy controls including privacy training to new hires;Assess risks in (b)(3) (b)(3):6(f),(b)(4)Consider changes in	(b)(3):6(f),(b)(4)		



Case	Strategic Business Unit	Project Name/Description	Project Start/End	Additional Information
	<p>the regulatory environment; and</p> <ul style="list-style-type: none">Consider the impact of any changes to MML operations or business arrangements (e.g., acquisitions, divestitures).	(b)(3):6(f),(b)(4)		
7.2-G	(b)(3):6(f),(b)(4)			



Item	Statement Description	Accounting Method	Reporting Period	Reporting Period
	(b)(3):6(f),(b)(4)			
7.2-M				



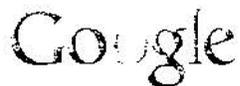
Code	Accounting Standards	Accounting Principles	Accounting Practices	Accounting Policies
7.3-G	(b)(3):6(f),(b)(4)			
7.3-M				
7.4-G				



REF.	Complete Contract Number	Project/Task/Requirement	Description/Status	Additional Information
	(b)(3):6(f),(b)(4)			
7.4-M				
7.5-G				



Ref.	Subject/Confidential Exclusion	Sensitivity/Classification	Access/Control	Authorized Information
7.5-M	(b)(3):6(f), (b)(4)			



Management's Assertion

The management of Google Inc. ("Google" or the "Company") represents that as of and for the two years ended April 25, 2014, and throughout the period August 1, 2013 to April 25, 2014 as it relates to Motorola Mobility LLC's ("Motorola" or "MML") privacy controls (the "Assessment 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 had established and implemented a comprehensive Privacy Program, (the "Google Privacy Program"), based on Company specific criteria (described in paragraph four 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 Assessment Period.

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

Furthermore, the Company represents that for the Assessment Period, the privacy controls within the Google Privacy Program as described on pages 20-54 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 on pages 20-54.

- 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

Sr. Privacy Counsel

Google Inc.

By:  _____

Lawrence You

Director of Privacy, Product and Engineering

Google Inc.



Appendix A – Assessment Interviews Summary

The following Google individuals were interviewed by PwC and/or provided evidence to support the above Assessment procedures.

Title	Team
(b)(3);6(f),(b)(4)	

Google Inc.
1600 Amphitheatre Parkway
Mountain View, CA 94043



Main 650.253.0000
Fax 650.253.0001
www.google.com

May 18, 2012

Via Certified Mail

Associate Director,
Division of Enforcement, Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, D.C. 20580

Re: In the Matter of Google Inc., FTC Docket No. C-4336

To the Associate Director of Enforcement:

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

Sincerely,

A handwritten signature in black ink, appearing to read "Keith Enright", written over a horizontal line.

Keith Enright
Senior Privacy Counsel
Google Inc.



HUNTON & WILLIAMS LLP
200 PARK AVENUE
NEW YORK, NY 10166-0005

TEL. 212 • 309 • 1000
FAX 212 • 309 • 1100

LISA J. SOTTO
DIRECT DIAL: 212 • 309 • 1223
EMAIL: lsotto@hunton.com

July 2, 2014

VIA EMAIL AND OVERNIGHT MAIL

James A. Kohm, Esq.
Associate Director
Division of Enforcement
Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

**Re: In the Matter of Google Inc., FTC Docket No. C-4336
Biennial Assessment Report on Google Inc.'s Privacy Program**

Dear Mr. Kohm:

Google Inc. ("Google") herewith submits its Biennial Assessment Report on Google's Privacy Program ("Assessment Report") in connection with the Decision and Order, Docket No. C-4336, issued by the Federal Trade Commission ("Commission"). The Assessment Report contains highly confidential and sensitive information regarding the design of Google's privacy program that is proprietary to Google. Public disclosure of this otherwise non-public information likely would result in substantial competitive harm and harm to Google's customers.

Google therefore requests that the Commission keep the designated portions of this Assessment Report confidential consistent with the Commission's Rules of Practice, 16 C.F.R. § 4.9(b)(7), (c); the relevant provisions of the Federal Trade Commission Act, 15 U.S.C. §§ 46(f), 57b-2(a-f); the relevant exemptions in the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552(b)(3), (4) and (7); and all other applicable statutes and regulations. In the event any third party seeks disclosure of or access to these materials, whether under FOIA or otherwise, Google requests to be timely notified by your office and given an opportunity to object to any such disclosure or grant of access, consistent with the Federal Trade Commission Act and the Commission's Rules of Practice. 15 U.S.C. § 57b-2(c); 16 C.F.R. §4.9(c)(1); 16 C.F.R. § 4.10(e). Furthermore, in the event your office discloses the Assessment Report to any third party, Google requests that you advise such third party of its highly confidential nature.



James A. Kohm, Esq.
July 2, 2014
Page 2

Accordingly, Google is submitting two versions of the Assessment Report: one version that appears in its entirety and another version that is redacted. Confidential portions of the redacted version are replaced with the word "redacted."

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

Very truly yours,

A handwritten signature in cursive script, appearing to read "Lisa J. Sotfo".

Lisa J. Sotfo

Enclosures

cc: Robin I. Moore, Esq. (w/enc.)
Keith Enright, Esq. (w/enc.)
Liz Eraker Palley, Esq. (w/enc.)