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

Mike Swift
MLex Market Intelligence
324 Metzgar Street
Half Moon Bay, CA 94019

SEP 26 2012

Re: FOIA-2012-01356
Third Party Privacy Report - Google

Dear Mr. Swift:

This is in response to your request dated September 13, 2012, under the Freedom of Information Act seeking access to the privacy report Pricewaterhouse Coopers, LLP created pursuant to the Google Buzz consent order, C-4336. In accordance with the FOIA and agency policy, we have searched our records, as of September 13, 2012, the date we received your request in our FOIA office.

We have located 34 pages of responsive records. I am granting partial access to and am enclosing copies of the accessible records. Four pages and portions of other pages fall within the exemptions to the FOIA's disclosure requirements, as explained below.

Some responsive records 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.

Based on the fee provisions of the FOIA, 5 U.S.C. § 552(a)(4)(A), and the Commission's Rules of Practice, 16 CFR § 4.8 et seq., as amended, I am not enclosing an invoice.

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 are handling your request or about the FOIA regulations or procedures, please contact Julian Chender at (202) 326-2631.

Sincerely,

Dione J. Stearns

Dione J. Stearns
Assistant General Counsel

Google

July 2, 2012

Associate Director of Enforcement
Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, DC 20580

Dear Associate Director of Enforcement:

Pursuant to Section IV of the Google Buzz Consent Order, *In the Matter of Google Inc.*, FTC Docket No. C-4336 (Oct. 28, 2011), Google hereby submits its Initial Assessment Report on Google's Privacy Program ("Assessment Report") prepared by third party Pricewaterhouse Coopers LLP.

As authorized by law, Google requests that the Commission keep the designated portions of the attached Assessment Report confidential pursuant to 16 C.F.R. § 4.9(c)(1). The enclosed request sets out the basis for confidential treatment.

I affirm under penalty of perjury under the laws of the United States of America that the attached is a true and correct copy of the Initial Assessment Report on Google's Privacy Program ("Assessment Report") prepared by third party Pricewaterhouse Coopers LLP. Executed on _____.

Sincerely,

Keith Enright
Google Inc.

Albert Gidari
PHONE: (206) 359-8688
FAX: (206) 359-9688
EMAIL: AGidari@perkinscoie.com

1201 Third Avenue, Suite 4800
Seattle, WA 98101-3099
PHONE: 206.359.8000
FAX: 206.359.9000
www.perkinscoie.com

July 3, 2012

Associate Director of Enforcement
Bureau of Consumer Protection
Federal Trade Commission
Washington, D.C. 20580

**Re: In the Matter of Google Inc., F.T.C. Docket No. C-4336; Confidentiality Request for Initial Assessment Report on Google Inc.'s Privacy Program**

Dear Associate Director of Enforcement:

Google Inc. ("Google") requests that the Commission keep confidential the designated portions of the Initial Assessment Report on Google's Privacy Program ("Assessment Report").

Commission rules permit "[p]ersons submitting material to the Commission described in this section" to "designate that material or portions of it [are] confidential and request that it be withheld from the public record." 16 C.F.R. § 4.9(c)(1). Sufficient evidence to grant a request for confidential treatment includes a showing that Google is likely to suffer substantial competitive harm, which can be demonstrated by showing that Google is (1) engaged in competition, (2) disclosure of the Assessment Report would result in a likelihood of substantial injury that (3) flows from a competitor's affirmative use of proprietary information. *See Public Citizen Health Research Group v. FDA*, 704 F.2d 1280, 1288 (D.C. Cir. 1983) (describing required showing to demonstrate confidential treatment under the Freedom of Information Act, 5 U.S.C. § 552(b)(4)); *Gulf & W. Indus. v. United States*, 615 F.2d 527 (D.C. Cir. 1980); *Nat'l Parks & Conservation Ass'n v. Morton*, 498 F.2d 765, 770 (D.C. Cir. 1974); *see also Gilda Indus. v. U.S. Customs & Border Protection Bureau*, 457 F. Supp. 2d 6, 9 (D.D.C. 2006).

This standard is met here. Google is engaged in competition. Much of the report describes the steps taken by Google to protect the privacy and confidentiality of user information and Google's internal procedures to do so. Disclosure of these steps and procedures necessarily compromises that goal, as well as causing commercial harm to Google and potentially its users. The Assessment Report contains detailed confidential and proprietary information regarding the design of Google's privacy program, including its impact on the development and review of products and services; the manner in which personal information is maintained within Google;

and related business processes. If disclosed, this otherwise non-public information could be easily used and exploited in an unfair manner by various competitors in the Internet service provider business seeking to harm Google commercially. Indeed, at least one of Google's fiercest competitors is subject to a similar consent decree requirement and the design of Google's privacy program is therefore competitively sensitive.

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

Google therefore requests that the Commission keep the designated portions of this Assessment Report confidential consistent with the Commission Rules, 16 C.F.R. § 4.9(b)(7), (c); the relevant provisions of the FTC Act, 15 U.S.C. §§ 46(f), 57b-2(a-f); FOIA exemptions three, four, and seven, 5 U.S.C. § 552(b)(3), (4), and (7); and all other applicable statutes, regulations, and customary confidentiality policies. Section 21(c)(1) of the FTC Act, 15 U.S.C. § 57b-2(c)(1), prohibits the Commission from disclosing information marked confidential except in accordance with Sections 21(c)(2) and (3); *see also* 15 U.S.C. § 57-b(2)(c)(2) (requiring the Commission to "notify such person in writing that the Commission intends to disclose the document at a date not less than 10 days after the date of receipt of the notification"); 15 U.S.C. § 57-b(2)(c)(3) (permitting a person to bring an action in United States District Court to restrain disclosure of materials pursuant to Section 21(c)(2)). In the event any third party (including any other governmental agency or body) seeks disclosure of, or access to, these materials, whether under FOIA or another context, 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 FTC Act and Commission Rules. 15 U.S.C. § 57-b2(c); 16 CFR § 4.9(c)(1); 16 CFR § 4.10(e). Furthermore, in the event that your office discloses the Assessment Report to any third party, Google requests that you advise such third party of its highly confidential nature.

Consistent with the Enforcement Bureau Instructions regarding the submission of confidential and proprietary trade secret business information, Google has submitted two copies of the Assessment Report: one copy in its entirety, and another "redacted" copy in which the confidential portions are redacted and replaced with the word 'redacted,' thereby preserving the original formatting of the document. *See* Letter from Katherine Robinson, Federal Trade Commission Enforcement Bureau, *In the Matter of Google Inc.*, FTC Docket No. C-4336 (Nov. 28, 2011) ("Enforcement Bureau Instructions").

Very truly yours,

Al Gidari /JRT

Albert Gidari

AG:JRT

pwc

# Initial Assessment Report
# on
# Google's Privacy Program

## For the period October 29, 2011 - April 25, 2012

pwc

Google Inc. ("the Company") has implemented and maintains a comprehensive Privacy Program, which is documented in written policies and procedures. Google has designated specific officials as responsible for the Privacy Program. On October 22, 2010, Dr. Alan Eustace, Senior Vice President of Engineering announced the appointment of Dr. Alma Whitten as the Director of Privacy across Engineering and Product Management. Dr. Whitten and her team lead Google's implementation of effective privacy controls in Google products and services. In his announcement, Dr. Eustace also noted that Google would enhance privacy training for engineers and other groups and that Technical Leads ("Tech Leads") would be "required to maintain a Privacy Design Document ("PDD") for each initiative they are working on."

In addition to the work of Dr. Whitten's 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 or service teams. Product Area Attorneys are responsible first and foremost for ensuring that any product or service complies with relevant legal requirements, including those relating to privacy. In addition, Google's legal department now 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 Documents 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 Programs across the organization, responsibility for privacy is in no way limited to any individual team. Many employees across teams and functions at Google are responsible for the Privacy Program in various respects.

The Privacy Program has a number of components and teams, collaborating to protect and improve the privacy of Google users, as well as working to promote compliance with the privacy related laws applicable to Google in the many jurisdictions within which Google operates. Two central aspects of the Privacy Program are the privacy innovation and protection efforts of the Product and Engineering team, and the privacy legal compliance efforts of the Privacy Legal team.

The 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;

pwc

4. Give users meaningful choices to protect their privacy; and
5. Be a responsible steward of the information Google holds.

PwC Assessor Qualifications

Section IV of the Federal Trade Commission ("FTC") Agreement Containing Consent Order ("the Order") requires that Google obtain an Assessment and report of its Privacy Program from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession ("the Assessment"). The Assessment was performed under professional standards which meet these same requirements.

PwC has one of the leading privacy practices in the United States and the world. Our dedicated teams of cross-disciplinary specialists help companies develop integrated approaches to privacy, security and information risk management. As a result, Forrester has recognized PwC as the number one privacy and security practice for three consecutive years, noting our integrated approach to privacy, compliance, security, and identity theft prevention as leading factors. In addition, ComputerWorld recognized PwC as tied for the top consulting firm with a privacy practice.

PwC's privacy compliance, information security, and risk management professionals hold leadership positions in many organizations that define privacy leading practices and standards. This exposure provides us deep knowledge of industry practices, procedures and standards as well as global regulatory requirements. Specifically, PwC is a founding member of the third-party Web Seal program TRUSTe, the International Association of Privacy Professionals (IAPP), and other industry groups. PwC specialists also have played leadership roles and drafted guidelines in organizations such as the Direct Marketing Association, Online Privacy Alliance, and the Privacy and American Business Chief Privacy Officer Program.

As one of the "Big 4" public accounting firms, 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") and by state societies of CPAs, state boards of accountancy, the Securities and Exchange Commission ("SEC"), and the Public Company Accounting Oversight Board ("PCAOB"). 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 Reporting Standards.

PwC assembled an experienced, cross-disciplinary team of PwC team members with privacy, FTC assessment, and industry experience to perform the Assessor role for the Google FTC Order.

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

pwc

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

Assessment and Reporting Standard

"Assurance" is a term defined by the International Framework for Assurance Engagements issued by the International Auditing and Assurance Standards Board ("IAASB") to mean "an engagement in which a practitioner expresses a conclusion designed to enhance the degree of confidence of the intended users other than the responsible party about the outcome of the evaluation or measurement of a subject matter against criteria." In other words, assurance that A (the subject matter) is presented in accordance with B (the criteria) (for example, A = the Google Privacy Program is presented in accordance with B = "Google specific criteria" defined in Attachment A of Management's Assertion on pages 19-24). The ability to perform an assurance engagement depends significantly on the appropriateness of A and the suitability of B as a measurement tool.

Assurance involves the testing of processes, systems, and data, as appropriate, and then assessing the findings in order to support an assurance conclusion, whether reasonable ("in our opinion, A is presented fairly, in all material respects, with B") or limited ("nothing came to our attention to indicate that A is not presented in accordance with B").

pwc

An attestation "examination" is similar to an audit, as it results in positive assurance (i.e., a "presents fairly, in all material respects" opinion) over the subject matter. The engagement is performed in accordance with AICPA Professional Attestation Standards, (b)(3):6(f),(b)(4) (b)(3):6(f),(b)(4)

In order to accept an assurance engagement, the AICPA's Professional Attestation Standards, (b) (b)(3):6(f),(b)(4)

(b)(3):6(f),(b)(4) criteria are the standards or benchmarks used to measure and present the subject matter and against which the practitioner evaluates the subject matter.

Suitable criteria must be objective, measurable, complete, and relevant. This means they should be free from bias and sufficiently complete so that any relevant factors omitted would not alter a conclusion about the subject matter. They also should permit reasonably consistent estimation or measurement of the subject matter from one company to another. This generally means that the criteria cannot be so subjective or vague that they are not capable of providing a reasonable basis for a meaningful conclusion.

Criteria may be external to the organization or developed internally, but must be readily available to the intended users of the assurance report. In most cases, there is no single authoritative source of criteria (such as generally accepted accounting principles or "GAAP" for financial statement assurance); therefore, the client needs to look to relevant regulations or frameworks, accepted industry standards, or its own internal policies and procedures when developing the criteria.

Independence

PwC is independent with respect to the professional standards required for this engagement. No other services provided to the Company impair our independence for purposes of this (b)(3):6(f), (b)(4) engagement.

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

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

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

pwc

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

Based on PwC's assessment procedures outlined above, the following section summarizes PwC's responses to parts A, B, C and D of Paragraph IV of the Order.

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

Google has utilized the company-defined criteria on pages 19-24 as the basis for its Privacy Program. As depicted on pages 19-24, Google has listed the privacy controls that were implemented and maintained during the reporting period.

Google has set forth the privacy controls that the Company has implemented and maintained during the reporting period. As described on pages 5-8, PwC performed test procedures to assess the effectiveness of the Google privacy controls implemented to meet or exceed the protections required by Paragraph III of the Order, and PwC's conclusions are on pages 14-15.

***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.***

Google's mission is to organize the world's information and make it universally accessible and useful. Google has grown from a company offering search, to offering a variety of services, including Gmail, Google Maps, Google Apps, Blogger, Chrome, Android, YouTube, and Google+, to users around the world. With worldwide headquarters in Mountain View, California, Google employs over 30,000 employs and has more than 70 offices in 40 countries around the world.

User data collected by Google can be generally described as belonging to one of three broad categories:

Log data: Log data is the record that Google keeps of a computer's interaction with Google's service. (b)(3):6(f),(b)(4)

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

pwc

Account data: Account data is the information stored in connection with a Google Account that a user has created. (b)(3):6(f),(b)(4)

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

(b)(3):6(f),(b)(4) The user can access this data, can delete this data, and can delete the account.

(b)(3):6(f),(b)(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. Refer to the response to letter "C" below for more information on the privacy risk assessment.

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 on pages 19-24 as the basis for its Privacy Program. These management assertions and privacy controls are intended to be implemented to meet the requirements identified by Google's privacy risk assessment, which Google performed to identify the applicable privacy risks and safeguards that needed to be implemented as part of its Privacy Program. This is considered to be an applicable set of criteria to address the Company's obligations within the Order.

As described above, Google established privacy controls that are appropriate to its size and complexity, the nature and scope of Respondent's activities, and the sensitivity of covered information. As described on pages 5-8, PwC performed test procedures to assess the effectiveness of the Google privacy controls implemented to meet or exceed the protections required by Paragraph III of the Order, and PwC's conclusions are on pages 14-15.

***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 controls on pages 19-24, Google has implemented the following protections:

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

Google has appointed Dr. Alma Whitten as the Director of Privacy across Engineering and Product Management. Dr. Whitten and her team lead Google's implementation of effective

privacy controls in Google products and services. In addition to the work of Dr. Whitten's 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 or service teams. Product Area Attorneys are responsible first and foremost for ensuring that any product or service complies with relevant legal requirements, including those relating to privacy. In addition, Google's legal department now has 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 Documents to identify privacy legal concerns, and to provide legal guidance and support regarding privacy law to other Google teams and employees as appropriate.

Privacy roles and responsibilities of employees and groups that play a part in privacy at Google are defined and published. (Google privacy control 2.1)

Google maintains an online privacy organizational chart and communication model. (Google privacy control 2.2)

Google publicly states the names, roles, and functions of privacy officials. (Google privacy control 2.3)

A working group of privacy related subject matter experts, the Privacy Working Group ("PWG"), provides oversight of privacy topics. (Google privacy control 2.4)

As described above, Google has designated employees to coordinate and be responsible for the Privacy Program as required by Paragraph III of the Order. As described on pages 5-8, PwC performed test procedures to assess the effectiveness of the Google privacy controls implemented to meet or exceed the protections required by Paragraph III of the Order, and PwC's conclusions are on pages 14-15.

*B. The identification of reasonably foreseeable, material risks, both internal and external, that could result in the 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.*

Privacy Risk Assessment

Pursuant to the Order's requirement that the respondent perform a privacy risk assessment, 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.

Google's privacy risk assessment process requires, at a minimum, that formal privacy risk assessments be completed by a cross-functional team of subject matter experts no less than once per year. The group responsible for the privacy risk assessment includes members of the Product and Engineering, Legal, Engineering Compliance, and Internal Audit teams. The Google privacy risk assessment process evaluates potential privacy risks and the sufficiency of existing controls. At the end of each risk assessment cycle, the privacy risk assessment team identifies areas of risk which might warrant additional mitigation, suggests additional or alternative mitigating controls to improve the risk posture of covered information, and escalates these control recommendations as appropriate for evaluation and implementation.

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

Privacy team reviews the Risk Assessment results, and identifies opportunities to further reduce or mitigate risk. (Google privacy control 3.2)

Risk Assessment results are communicated to management in a timely manner. (Google privacy control 3.3)

As described 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 Paragraph III of the Order. As described on pages 5-8, PwC performed test procedures to assess the effectiveness of the Google privacy controls implemented to meet or exceed the protections required by Paragraph III of the Order, and PwC's conclusions are on pages 14-15.

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

Design & Implementation of Safeguards

Based on the risks identified through the privacy risk assessment described in B. above, Google designed and implemented the privacy controls documented on pages 19-24.

pwc

Regular Testing & Monitoring of Safeguards

Google regularly tests or monitors the effectiveness of its privacy controls. (b)(3):6(f),(b)(4)

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

As described above, Google has designed and implemented reasonable privacy controls and procedures to address the risks identified through the privacy risk assessment, and regular testing or monitoring of the effectiveness of those privacy controls and procedures as required by Paragraph III of the Order. As described on pages 5-8, PwC performed test procedures to assess the effectiveness of the Google privacy controls implemented to meet or exceed the protections required by Paragraph III of the Order, and PwC's conclusions are on pages 14-15.

*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 contract with service providers capable of appropriately protecting and maintaining the privacy of covered information received from Google. Google also includes terms in contracts with service providers requiring that such service providers implement and maintain appropriate privacy protections.

Selection of Service Providers

The Ethics & Compliance team reviews purchase requisitions and refers service providers to the Vendor Security Audit (VSA) team based on risk. (Google privacy control 6.1)

Service providers are required to sign confidentiality terms as part of the agreement. (Google privacy control 6.3)

VSA team performs a review of service providers according to risk-based process. (Google privacy control 6.4)

pwc

Retention of Service Providers
Privacy related risks are considered and documented as part of scoping and execution for vendor audits performed by Internal Audit. (Google privacy control 6.6)

As described above, Google has developed and used reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from Google, and requiring service providers by contract to implement and maintain appropriate privacy protections as required by Paragraph III of the Order. As described on pages 5-8, PwC performed test procedures to assess the effectiveness of the Google privacy controls implemented to meet or exceed the protections required by Paragraph III of the Order, and PwC's conclusions are on pages 14-15.

*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.*

Given the changing nature of privacy threats, and the constant evolution of Google's business practices, Google implements improved privacy controls over time, and retires legacy controls if they are no longer deemed useful or justified in mitigating privacy risk. (b)(3):6(f),(b)(4)
(b)(3):6(f),(b)(4)

As described above, Google has evaluated and adjusted its Privacy Program in light of the results of the testing and monitoring required by subpart C within paragraph III, any material changes to Google's operations or business arrangements, or any other circumstances that Google knows or has reason to know may have a material impact on the effectiveness of its Privacy Program as required by Paragraph III of the Order. As described on pages 5-8, PwC performed test procedures to assess the effectiveness of the Google privacy controls implemented to meet or exceed the protections required by Paragraph III of the Order, and PwC's conclusions are on pages 14-15.

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

As described in the PwC Assessment Overview section above, PwC performed its assessment of Google's Privacy Program in accordance with AICPA Attestation Standards (b)(3):6(f),(b)(4)
(b)(3):6(f),(b)(4) Refer to pages 14-15 for PwC's conclusions.

pwc

## Report of Independent Accountants

To the Management of Google, Inc.:

We have examined Management's Assertion, included in the accompanying Exhibit I, that as of and for the six month period ended April 25, 2012 (the "Reporting Period"), in accordance with Parts III and IV of the Agreement Containing Consent Order ("the Order") with a service date of October 28, 2011, between Google ("the Company") and the Federal Trade Commission ("FTC"), that the Company had: (i) established and implemented a comprehensive privacy program, based on Company specific criteria detailed in Attachment A (collectively referred to as the "Google Privacy Program"), and, (ii) the privacy controls were operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the Reporting Period.

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

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

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 reporting period, in all material respects as of and for the six months ended April 25, 2012, based upon the Google Privacy Program set forth in Attachment A of Management's Assertion in Exhibit I.

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

pwc

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 22, 2012

Our initial assessment report constitutes and reflects work performed or information obtained by PricewaterhouseCoopers LLP, in our capacity as independent assessor for Google for the purpose of the Google FTC Agreement and Order. The report contains trade secrets and confidential commercial information of our firm and Google that is privileged and confidential, and we expressly reserve all rights with respect to disclosures to third parties. Accordingly, we request confidential treatment under the Freedom of Information Act (FOIA) 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 there from. We further request that written notice be given to our firm before distribution of the information in the report (or copies thereof) to others, including other governmental agencies, to afford our firm and Google 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 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.

Google

## Exhibit I

## Management's Assertion

The management of Google Inc. ("the Company") represents that as of and for the six month period ended April 25, 2012 ("the Reporting Period"), in accordance with Parts III and IV of the Agreement Containing Consent Order ("the Order") with a service date of October 28, 2011, between the Company and the Federal Trade Commission ("FTC"), the Company had: (i) established and implemented a comprehensive privacy program, based on Company specific criteria detailed in Attachment A (collectively referred to as the "Google Privacy Program"), and, (ii) the privacy controls were operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the Reporting Period, in accordance with Part III C of the Order.

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

Google Inc.

By: _____
Mr. Keith Enright
Senior Privacy Counsel

By: _____
Dr. Alma Whitten
Director, Privacy Engineering & Product Management

Google

**Attachment A to Management's Assertion: Google Privacy Program**

This attachment describes the scope of the Google Privacy Program referenced in the management assertion on the previous page.

Google's mission is to organize the world's information and make it universally accessible and useful. The company, which began as a search engine, was founded in 1998 by Larry Page and Sergey Brin. Since then, Google has grown from a company offering search, to offering a variety of services, including Gmail, Google Maps, Google Apps, Blogger, Chrome, Android, YouTube, and Google+, to users around the world.

Google has implemented and maintains a comprehensive privacy program, referred to herein as the Privacy Program, which is documented in written policies and procedures. Google has designated specific officials as responsible for the Privacy Program. While designated employees carry leadership responsibility for coordinating the privacy innovation and compliance efforts across the organization, responsibility for privacy is in no way limited to any individual team. Many employees across teams and functions at Google are responsible for the Privacy Program in various respects.

The Privacy Program has a number of components and teams, collaborating to protect and improve the privacy of Google users, as well as working to promote compliance with the privacy-related laws applicable to Google in the many jurisdictions within which Google operates. Two central aspects of the Privacy Program are the privacy innovation and protection efforts of the Product and Engineering team, and the privacy legal compliance efforts of the Privacy Legal team.

The 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 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.

On October 22, 2010, Google announced a substantial expansion of its Privacy Program, including a key executive appointment and a number of important privacy controls. Dr. Alan Eustace, Senior Vice President of Engineering at that time, announced the appointment of Dr. Alma Whitten as the Director of Privacy across Engineering and Product Management. Dr. Whitten and her team lead Google's implementation of effective privacy controls in our products and services. In his announcement, Dr. Eustace also noted that Google would enhance privacy training for engineers and other groups and that Tech Leads would be "required to maintain a privacy design document for each initiative they are working on."

In addition to the work of Dr. Whitten's 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 or service teams. Product Area Attorneys are responsible first and foremost for ensuring that any product or service complies with relevant legal requirements, including those relating to privacy. In addition, Google's legal department now has 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 Documents (as described below) to identify privacy legal concerns, and to provide legal guidance and support regarding privacy law to other Google teams and employees as appropriate.

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 in order to identify reasonably foreseeable, material privacy 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. Refer to pages 19-24 below for a list of Google's privacy assertions and controls identified as a result of the privacy risk assessment.

Google's privacy risk assessment process requires, at a minimum, that formal privacy risk assessments be completed by a cross-functional team of subject matter experts no less than once per year. The group responsible for the privacy risk assessment includes members of the Product and Engineering, Legal, Engineering Compliance, and Internal Audit teams. The Google privacy risk assessment process evaluates potential privacy risks and the sufficiency of existing controls. At the end of each risk assessment cycle, the privacy risk assessment team identifies areas of risk which might warrant additional mitigation, suggests additional or alternative mitigating controls to improve the risk posture of covered information, and escalates these control recommendations as appropriate for evaluation and implementation. Consistent with the requirement of the Order that Google implement "controls and procedures appropriate to ... the sensitivity of covered information," the Reporting Period did not include events that would suggest that the Privacy Program failed to provide a reasonable level of assurance to protect the privacy of covered information.

Google

## Google Management Assertions and Supporting Privacy Controls

| Control Ref # | Google Privacy Control Description | Consent, Use and/or Disclosure |
|---|---|---|
| **Assertion 1.**<br><br>**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. | Consent<br>Use<br>Disclosure |
| 1.2 | The Privacy Program is periodically reviewed for appropriateness. | Consent<br>Use<br>Disclosure |
| 1.3 | Internal privacy policies are periodically reviewed for consistency with external privacy policies and updated as necessary. | Consent<br>Use<br>Disclosure |
| **Assertion 2.**<br><br>**Google has designated specific employees as officials responsible for Google's Privacy Program.** | | |
| 2.1 | Privacy roles and responsibilities of employees and groups that play a part in privacy at Google are defined and published. | Consent<br>Use<br>Disclosure |
| 2.2 | Google maintains an online privacy organizational chart and communication model. | Consent<br>Use<br>Disclosure |
| 2.3 | Google publicly states the names, roles, and functions of privacy officials. | Consent<br>Use<br>Disclosure |
| 2.4 | A working group of privacy related subject matter experts, Privacy Working Group ("PWG"), provides oversight of privacy topics. | Consent<br>Use<br>Disclosure |
| **Assertion 3.**<br><br>**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.** | | |

Google

| | | |
|---|---|---|
| 3.1 (7.1) | (b)(3):6(f),(b)(4) | Consent<br>Use<br>Disclosure |
| 3.2 (7.4) | Privacy team reviews the Risk Assessment results, and identifies opportunities to further reduce or mitigate risk. | Consent<br>Use<br>Disclosure |
| 3.3 | Risk Assessment results are communicated to management in a timely manner. | Consent<br>Use<br>Disclosure |
| **Assertion 4.**<br><br>**On an ongoing basis, Google implements reasonable privacy controls and procedures to address identified privacy risks.** | | |
| 4.1 | PDDs are required to be completed and reviewed throughout the product development life cycle. | Consent<br>Use<br>Disclosure |
| 4.2 | Google facilitates transparency & choice by providing end-user privacy settings which include:<br>* Dashboards: Account Dashboard, Account Central, Account Activity, Latitude Dashboard, Gov Requests Dashboard<br>* Social Settings: G+ Visibility Inspector, sharing ACLs, Circles<br>* Ads Settings: Ads Preferences Manager<br>* Confidentiality: SSL on Gmail & Search<br>* Data Portability: Data Liberation, deletion | Consent<br>Use<br>Disclosure |
| 4.3 | (b)(3):6(f),(b)(4) | Consent<br>Use<br>Disclosure |
| 4.4 | (b)(3):6(f),(b)(4) | Consent<br>Use<br>Disclosure |

Google

| | | |
|---|---|---|
| | (b)(3):6(f),(b)(4) | |
| 4.5 | | *Unused control reference* |
| 4.6 | | Consent<br>Use<br>Disclosure |
| 4.7 | | Consent<br>Use<br>Disclosure |
| 4.8 | | Consent<br>Use<br>Disclosure |
| 4.9 | Employees are required to complete Ethics & Compliance code of conduct training, which includes reference to privacy policies, (b)(3):6(f),(b)(4) (b)(3):6(f), | Consent<br>Use<br>Disclosure |
| 4.10 | (b)(3):6(f),(b)(4) | Consent<br>Use<br>Disclosure |
| 4.11 | | Consent<br>Use<br>Disclosure |
| 4.12 | | Consent<br>Use<br>Disclosure |
| 4.13 | | Consent<br>Use<br>Disclosure |
| 4.14 | | Consent<br>Use<br>Disclosure |
| 4.15 | | Use<br>Disclosure |

Google

| | | |
|---|---|---|
| | (b)(3):6(f),(b)(4) | |
| 4.16 | *Unused control reference* | *Unused control reference* |
| 4.17 | *Unused control reference* | *Unused control reference* |
| 4.18 | *Unused control reference* | *Unused control reference* |
| 4.19 | *Unused control reference* | *Unused control reference* |
| 4.20 | (b)(3):6(f),(b)(4) | Use<br>Disclosure |
| 4.21 | | Use<br>Disclosure |
| 4.22 | | Use<br>Disclosure |
| 4.23 | Google maintains a site containing links to each of its privacy policies, and supplemental reference materials explaining its policies, at http://www.google.com/privacy[1]. | Consent<br>Use<br>Disclosure |
| **Assertion 5.**<br><br>**Google regularly tests or monitors the effectiveness of the privacy controls.** | | |
| 5.1 | (b)(3):6(f),(b)(4) | Consent<br>Use<br>Disclosure |
| 5.2 (7.5) | | Consent<br>Use<br>Disclosure |
| 5.3 | | Consent<br>Use<br>Disclosure |
| 5.4 | | Consent<br>Use<br>Disclosure |
| 5.5 | *Unused control reference* | *Unused control reference* |

Google

| | | |
|---|---|---|
| 5.6 | *Unused control reference* | *Unused control reference* |
| 5.7 | *Unused control reference* | *Unused control reference* |
| **Assertion 6.**<br><br>**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 Ethics & Compliance team reviews purchase requisitions and refers service providers to the Vendor Security Audit (VSA) team based on risk. | Consent<br>Use<br>Disclosure |
| 6.2 | *Unused control reference* | *Unused control reference* |
| 6.3 | Service providers are required to sign confidentiality terms as part of the agreement. | Use<br>Disclosure |
| 6.4 | VSA team performs a review of service providers according to risk-based process | Consent<br>Use<br>Disclosure |
| 6.5 | *Unused control reference* | *Unused control reference* |
| 6.6 | Privacy related risks are considered and documented as part of scoping and execution for vendor audits performed by Internal Audit. | Consent<br>Use<br>Disclosure |
| **Assertion 7.**<br><br>**Google's 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 Privacy Program.** | | |
| 7.1 (3.1) | (b)(3):6(f),(b)(4) | Consent<br>Use<br>Disclosure |
| 7.2 | | Consent |

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

Google

## Policies & Principles

# Privacy Policy

Last modified: March 1, 2012 (view archived versions)

There are many different ways you can use our services – to search for and share information, to communicate with other people or to create new content. When you share information with us, for example by creating a Google Account, we can make those services even better – to show you more relevant search results and ads, to help you connect with people or to make sharing with others quicker and easier. As you use our services, we want you to be clear how we're using information and the ways in which you can protect your privacy.

Our Privacy Policy explains:

- What information we collect and why we collect it.
- How we use that information.
- The choices we offer, including how to access and update information.

We've tried to keep it as simple as possible, but if you're not familiar with terms like cookies, IP addresses, pixel tags and browsers, then read about these key terms first. Your privacy matters to Google so whether you are new to Google or a long-time user, please do take the time to get to know our practices – and if you have any questions contact us.

### Information we collect

We collect information to provide better services to all of our users – from figuring out basic stuff like which language you speak, to more complex things like which ads you'll find most useful or the people who matter most to you online.

We collect information in two ways:

- **Information you give us.** For example, many of our services require you to sign up for a Google Account. When you do, we'll ask for personal information, like your name, email address, telephone number or credit card. If you want to take full advantage of the sharing features we offer, we might also ask you to create a publicly visible Google Profile, which may include your name and photo.
- **Information we get from your use of our services.** We may collect information about the services that you use and how you use them, like when you visit a website that uses our advertising services or you view and interact with our ads and content. This information includes:
    - **Device information**

      We may collect device-specific information (such as your hardware model, operating system version, unique device identifiers, and mobile network information including phone number). Google may associate your device identifiers or phone number with your Google Account.

    - **Log information**

      When you use our services or view content provided by Google, we may automatically collect and store certain information in server logs. This may include:

- details of how you used our service, such as your search queries.
- telephony log information like your phone number, calling-party number, forwarding numbers, time and date of calls, duration of calls, SMS routing information and types of calls.
- Internet protocol address.
- device event information such as crashes, system activity, hardware settings, browser type, browser language, the date and time of your request and referral URL.
- cookies that may uniquely identify your browser or your Google Account.

- **Location information**

  When you use a location-enabled Google service, we may collect and process information about your actual location, like GPS signals sent by a mobile device. We may also use various technologies to determine location, such as sensor data from your device that may, for example, provide information on nearby Wi-Fi access points and cell towers.

- **Unique application numbers**

  Certain services include a unique application number. This number and information about your installation (for example, the operating system type and application version number) may be sent to Google when you install or uninstall that service or when that service periodically contacts our servers, such as for automatic updates.

- **Local storage**

  We may collect and store information (including personal information) locally on your device using mechanisms such as browser web storage (including HTML 5) and application data caches.

- **Cookies and anonymous identifiers**

  We use various technologies to collect and store information when you visit a Google service, and this may include sending one or more cookies or anonymous identifiers to your device. We also use cookies and anonymous identifiers when you interact with services we offer to our partners, such as advertising services or Google features that may appear on other sites.

## How we use information we collect

We use the information we collect from all of our services to provide, maintain, protect and improve them, to develop new ones, and to protect Google and our users. We also use this information to offer you tailored content – like giving you more relevant search results and ads.

We may use the name you provide for your Google Profile across all of the services we offer that require a Google Account. In addition, we may replace past names associated with your Google Account so that you are represented consistently across all our services. If other users already have your email, or other information that identifies you, we may show them your publicly visible Google Profile information, such as your name and photo.

When you contact Google, we may keep a record of your communication to help solve any issues you might be facing. We may use your email address to inform you about our services, such as letting you know about upcoming changes or improvements.

We use information collected from cookies and other technologies, like pixel tags, to improve your user experience and the overall quality of our services. For example, by saving your language preferences, we'll be able to have our services appear in the language you prefer. When showing you tailored ads, we will not associate a cookie or anonymous identifier with sensitive categories, such as those based on race, religion, sexual orientation or health.

We may combine personal information from one service with information, including personal information, from other Google services – for example to make it easier to share things with people you know. We will not combine DoubleClick cookie information with personally identifiable information unless we have your opt-in consent.

We will ask for your consent before using information for a purpose other than those that are set out in this Privacy Policy.

Google processes personal information on our servers in many countries around the world. We may process your personal information on a server located outside the country where you live.

## Transparency and choice

People have different privacy concerns. Our goal is to be clear about what information we collect, so that you can make meaningful choices about how it is used. For example, you can:

- Review and control certain types of information tied to your Google Account by using Google Dashboard.
- View and edit your ads preferences, such as which categories might interest you, using the Ads Preferences Manager. You can also opt out of certain Google advertising services here.
- Use our editor to see and adjust how your Google Profile appears to particular individuals.
- Control who you share information with.
- Take information out of many of our services.

You may also set your browser to block all cookies, including cookies associated with our services, or to indicate when a cookie is being set by us. However, it's important to remember that many of our services may not function properly if your cookies are disabled. For example, we may not remember your language preferences.

## Information you share

Many of our services let you share information with others. Remember that when you share information publicly, it may be indexable by search engines, including Google. Our services provide you with different options on sharing and removing your content.

## Accessing and updating your personal information

Whenever you use our services, we aim to provide you with access to your personal information. If that information is wrong, we strive to give you ways to update it quickly or to delete it – unless we have to keep that information for legitimate business or legal purposes. When updating your personal information, we may ask you to verify your identity before we can act on your request.

We may reject requests that are unreasonably repetitive, require disproportionate technical effort (for example, developing a new system or fundamentally changing an existing practice), risk the privacy of others, or would be extremely impractical (for instance, requests concerning information residing on backup tapes).

Where we can provide information access and correction, we will do so for free, except where it would require a disproportionate effort. We aim to maintain our services in a manner that protects information from accidental or malicious destruction. Because of this, after you delete information from our services, we may not immediately delete residual copies from our active servers and may not remove information from our backup systems.

## Information we share

We do not share personal information with companies, organizations and individuals outside of Google unless one of the following circumstances apply:

- **With your consent**

  We will share personal information with companies, organizations or individuals outside of Google when we have your consent to do so. We require opt-in consent for the sharing of any sensitive personal information.

- **With domain administrators**

  If your Google Account is managed for you by a domain administrator (for example, for Google Apps users) then your domain administrator and resellers who provide user support to your organization will have access to your Google Account information (including your email and other data). Your domain administrator may be able to:

  - view statistics regarding your account, like statistics regarding applications you install.
  - change your account password.
  - suspend or terminate your account access.
  - access or retain information stored as part of your account.
  - receive your account information in order to satisfy applicable law, regulation, legal process or enforceable governmental request.
  - restrict your ability to delete or edit information or privacy settings.

  Please refer to your domain administrator's privacy policy for more information.

- **For external processing**

  We provide personal information to our affiliates or other trusted businesses or persons to process it for us, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures.

- **For legal reasons**

  We will share personal information with companies, organizations or individuals outside of Google if we have a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary to:

  - meet any applicable law, regulation, legal process or enforceable governmental request.
  - enforce applicable Terms of Service, including investigation of potential violations.
  - detect, prevent, or otherwise address fraud, security or technical issues.
  - protect against harm to the rights, property or safety of Google, our users or the public as required or permitted by law.

We may share aggregated, non-personally identifiable information publicly and with our partners – like publishers, advertisers or connected sites. For example, we may share information publicly to show trends about the general use of our services.

If Google is involved in a merger, acquisition or asset sale, we will continue to ensure the confidentiality of any personal information and give affected users notice before personal information is transferred or becomes subject to a different privacy policy.

## Information security

We work hard to protect Google and our users from unauthorized access to or unauthorized alteration, disclosure or destruction of information we hold. In particular:

- We encrypt many of our services using SSL.
- We offer you two step verification when you access your Google Account, and a Safe Browsing feature in Google

Chrome.

- We review our information collection, storage and processing practices, including physical security measures, to guard against unauthorized access to systems.
- We restrict access to personal information to Google employees, contractors and agents who need to know that information in order to process it for us, and who are subject to strict contractual confidentiality obligations and may be disciplined or terminated if they fail to meet these obligations.

## Application

Our Privacy Policy applies to all of the services offered by Google Inc. and its affiliates, including services offered on other sites (such as our advertising services), but excludes services that have separate privacy policies that do not incorporate this Privacy Policy.

Our Privacy Policy does not apply to services offered by other companies or individuals, including products or sites that may be displayed to you in search results, sites that may include Google services, or other sites linked from our services. Our Privacy Policy does not cover the information practices of other companies and organizations who advertise our services, and who may use cookies, pixel tags and other technologies to serve and offer relevant ads.

## Enforcement

We regularly review our compliance with our Privacy Policy. We also adhere to several self regulatory frameworks. When we receive formal written complaints, we will contact the person who made the complaint to follow up. We work with the appropriate regulatory authorities, including local data protection authorities, to resolve any complaints regarding the transfer of personal data that we cannot resolve with our users directly.

## Changes

Our Privacy Policy may change from time to time. We will not reduce your rights under this Privacy Policy without your explicit consent. We will post any privacy policy changes on this page and, if the changes are significant, we will provide a more prominent notice (including, for certain services, email notification of privacy policy changes). We will also keep prior versions of this Privacy Policy in an archive for your review.

## Specific product practices

The following notices explain specific privacy practices with respect to certain Google products and services that you may use:

- Chrome and Chrome OS
- Books
- Wallet