Submitted to: DEbrief@ftc.gov

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

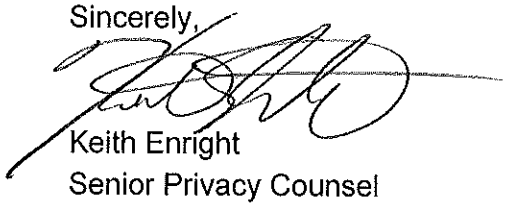
Re: In the Matter of Google Inc., FTC Docket No. C-4336

To the Associate Director of Enforcement:

Google Inc. ("Google") submits the attached Report as required by Part VIII of the Agreement Containing Consent Order ("Order"). The Report describes the steps Google has taken to comply with the Order. Per the instructions in your November 28, 2011, letter, the Report follows the outline of the Order paragraph by paragraph.

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

Sincerely,



Keith Enright
Senior Privacy Counsel
Google Inc.

In the Matter of *GOOGLE INC.,* *a Corporation.*	)))))))	**90 Day Report** **Docket No. C-4336**

The following Report is made pursuant to Part VIII of the Agreement Containing Consent Order ("Order") and describes the steps Google has taken to comply with the Order. The Report follows the outline of the Order paragraph by paragraph.

I.

Respondent, in or affecting commerce, shall not misrepresent in any manner, expressly or by implication:

A. the extent to which respondent maintains and protects the privacy and confidentiality of any covered information, including, but not limited to, misrepresentations related to: (1) the purposes for which it collects and uses covered information, and (2) the extent to which consumers may exercise control over the collection, use, or disclosure of covered information.

B. the extent to which respondent is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy, security, or any other compliance program sponsored by the government or any other entity, including, but not limited to, the U.S.-EU Safe Harbor Framework.

Google's comprehensive privacy program, described in greater detail and referred to as the "Privacy Effort" subsequently in this Report, reasonably assures that Google is acting in a manner consistent with its public representations regarding the privacy and confidentiality of covered information.

Google accurately describes the purposes for which it collects and uses covered information in its privacy policy, available at https://www.google.com/intl/en/policies/privacy/. This policy also identifies certain privacy compliance programs in which Google participates. Google's ongoing efforts to simplify, update and consolidate this privacy policy occasionally lead to

revisions. The most recent such revision was posted on Google.com on January 24, 2012, and will go into effect on March 1, 2012 (the "Effective Date"). No new or additional third party sharing is permitted under this revised policy beyond that which would have been permitted under the prior policy. Google has gone to exceptional lengths to notify users of this updated privacy policy so that they might review its terms and understand how Google collects, uses, and shares information from or about users. This notification effort is the largest user-facing notification effort Google has ever undertaken, for any reason, and includes five elements:

1. An email will be sent to every Google Account holder, except accounts associated with enterprise (Google Apps) customers. A separate email will be sent to the registered administrators of Google Apps domains, so that they may notify their users as they see fit. New accounts (created after January 24), will receive an email on the Effective Date.

2. Google will show a specific login interstitial to each Google Account holder at first login (except enterprise customer accounts, API users and mobile app users where this is not technically practicable). Only clicking on "OK, got it" or "Learn more" will dismiss the interstitial, otherwise it will persist. Users logging in for the first time only after the Effective Date will also see the interstitial until they choose an option.

3. Google will run a homepage promotion on Google.com (and other top-level-domains) for five days from the launch date. The text will not be dismissable.

4. "In-product notifications" will be displayed only on key unauthenticated properties. This includes all search results pages which are served from Google Web Server (but not the Google homepage), including on mobile (including Google Maps search results, Google News, iGoogle, mobile search and YouTube). All signed-out users will see the in-product notification (beginning January 24th), until clicking one of the links. After they clear the in-product notification (as long as they don't clear cookies), they will not see it again on the top level domain. As a further backstop measure, from February 6th onwards, Google will also show in-product notifications to signed-in Google Account users who have not gone through a login event in the past 14 days.

5. "New" footers will be displayed on (1) the Google homepage, (2) the "About" and other static corporate pages, (3) All results pages that are served from Google Web Server (i.e. web search, images, etc.), and (4) YouTube.

This aggressive notification process is designed to promote user awareness of the current terms of the Google Privacy Policy and to present users with clear information in order to exercise meaningful choice regarding their continued use of Google services in accordance with the Privacy Principles (defined below in Part III A).

II.

Respondent, prior to any new or additional sharing by respondent of the Google user's identified information with any third party, that: 1) is a change from stated sharing practices in effect at the time respondent collected such information, and 2) results from any change, addition, or enhancement to a product or service by respondent, in or affecting commerce, shall:

A. Separate and apart from any final "end user license agreement," "privacy policy," "terms of use" page, or similar document, clearly and prominently disclose: (1) that the Google user's information will be disclosed to one or more third parties, (2) the identity or specific categories of such third parties, and (3) the purpose(s) for the respondent's sharing; and

B. Obtain express affirmative consent from the Google user to such sharing.

Google has implemented a program to ensure the requirements of this Part II of the Order are followed. When this Part of the Order is triggered by a change in practices that would result in additional third-party sharing of a Google user's identified information, Google clearly and prominently explains that such information will be disclosed, to whom it will be disclosed and the purpose of such sharing, and obtains affirmative consent prior to such disclosure.

Google has sought to reinforce the third-party sharing provisions of the Order in a number of ways. First, these requirements have been communicated to Google management and to new employees. As required by the Order, the Order has been provided to every Google employee with supervisory responsibility relevant to the subject matter of the Order. As new employees are hired into such roles or existing employees are promoted into such positions, a copy of the Order is provided to them within 30 days of their date of hire or promotion. Second, distribution of the Order will be further supported by additional training and awareness efforts for employees in the future. As described in greater detail below, Google has launched a number of privacy training initiatives, many of which include materials describing the requirements of this Part so that employees understand both the triggers of the requirement and the specific notice and consent requirements. Third, Google's privacy review process, described in more detail in response to Part III C, is designed to identify new or changed products or services that may trigger the requirements of this Part II.

III.

Respondent, in or affecting commerce, shall, no later than the date of service of this order, 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. Such program, the content and implementation of which must be documented in writing, shall contain privacy controls and procedures appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the covered information, including:

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

Google has implemented and maintains a comprehensive privacy program, referred to herein as the Privacy Effort, which is documented in written policies and procedures. Google has designated specific officials as responsible for the Privacy Effort. 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 Effort in various respects.

The Privacy Effort 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 Effort 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 Effort 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 all 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 Effort. 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.

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, the 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.

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, IT Compliance, and Internal Audit teams. Google may adjust the frequency of such assessments in the future to optimize the risk management benefit of the process. 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.

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.

On an ongoing basis, Google implements reasonable privacy controls and procedures to address identified privacy risks. Google regularly tests or monitors the effectiveness of these privacy controls. 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.

Google's current privacy controls include, but are not limited to: the privacy design document ("PDD") review process, Product Area Attorneys legal review of projects prior to launch, and multiple types and levels of training to ensure that privacy issues are promptly recognized and that appropriate escalation paths and response protocols are consistently followed.

The Privacy Design Document Review Process

Within Google, "Tech Leads" are engineers responsible for a project as a whole, including setting the technical direction, coordinating activities, and acting as the main engineering representative of the project to other teams. Tech Leads must maintain a PDD for each project they work on. A PDD is a concise and straightforward document that clearly describes the types of data that are to be collected, handled, or processed, and how that data will be appropriately used and protected.

PDDs are submitted to and reviewed by members of a group known as the Privacy Working Group (or PWG), which includes representatives from Engineering, Product, User Experience (UX), Policy, Communications, Legal, and Compliance. This group flags and prioritizes projects for additional review based on privacy risk. Additional review may be limited to asking clarifying questions in instances where the project at issue carries minimal privacy risk, or may be as in-depth as having engineers from the Privacy Code Audit group verify the implementation where the underlying product or service substantially involves sensitive information.

Privacy Legal Review

Each Google product is assigned a Product Area Attorney who works with the product team to promote compliance with relevant regulations and laws. Product Area Attorneys, with support from Privacy Counsel with privacy law subject matter expertise, work with the product teams to identify and address privacy legal risks in products at an early stage. Throughout the design process, Product Area Attorneys provide the necessary legal advice to product teams to consider what types of information are being collected, how that information is used, whether that data will be shared and how it will be managed and secured.

Prior to launch, Product Area Attorneys work with the Privacy Legal team to ensure that

relevant privacy policies and terms of service meet applicable standards by being clear, accurate and legally sufficient as well as to ensure that the product includes an appropriate level of user notification and consent where needed.

Privacy Training

Google has implemented an array of training and awareness activities to promote recognition and understanding of privacy issues with respect to user information. Some of these activities are high-level and delivered to a very large audience, where the primary intention is to promote general privacy awareness and familiarize employees with important key concepts such as the Google Privacy Principles. Other training activities are more narrowly targeted to employees with responsibilities that may more substantially impact user privacy. The following non-exhaustive list outlines some of Google's privacy training activities to date.

1. New employees receive high-level privacy awareness training, including training regarding the Google Privacy Principles and the importance of user privacy to Google.

2. Employees at manager level or above are provided with a copy of the Order. They are encouraged to review the Order and reach out to the Legal Privacy team if they have any questions regarding its requirements.

3. Technical employees attend "Innovation in Privacy" training, delivered by a subject-matter expert from Dr. Whitten's team. The course teaches the importance of designing products with privacy in mind and how to properly complete PDDs.

4. Employees complete information security training. Though not privacy-specific training *per se*, this training advances each employee's ability to be a responsible steward of user information, as required by Google's Privacy Principles.

5. Engineers and engineering product managers are encouraged to complete "Advanced Data Protection" training, delivered by a subject matter expert from Dr. Whitten's team. This training is intended to promote a deeper understanding of how to build products that reflect Google's Privacy Principles.

6. Interactive "PM Privacy Workshops" are offered to improve product managers' ability to make informed privacy decisions for their products.

7. In cooperation with the International Association of Privacy Professionals (IAPP), Google has begun piloting privacy training based on the core curriculum supporting the Certified Information Privacy Professional (CIPP) certification. Beginning with a limited pilot in November 2011, with a second session completed in Google's Mountain View, California headquarters in January of 2012, these optional training sessions present much of the

standard body of knowledge required for the CIPP certification. Open to Google employees across a wide array of roles and responsibilities, these training sessions not only present a global view of privacy issues beyond Google, but also prepare Google employees to pursue the CIPP certification, if they choose to do so.

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 includes terms in contracts with service providers requiring that such service providers implement and maintain appropriate privacy protections.

Assessment of Service Providers

Google has developed and implemented a program to assess whether Google service providers are capable of appropriately protecting user information. Google has adopted written policies that require Google's Vendor Security Audit (VSA) team, as well as Legal and Privacy teams, as appropriate, to review service providers with access to a range of data, including users' personally identifiable information. This requirement is specifically reiterated in a number of places in Google's internal policies.

Google's VSA team maintains an internal website to provide guidance to personnel about when and how to engage the vendor assessment process. Service providers are first asked to respond to a preliminary pre-qualification questionnaire to determine whether the service provider has implemented reasonable safeguards for sensitive data. The providers' responses to pre-qualification questions are used to determine whether the service provider under review is capable of passing a comprehensive assessment.

The full VSA assessment requires that the service provider under review complete an in-depth questionnaire that probes the details of the provider's data protection program and controls. The VSA team then reviews the service provider's responses along with any available documentation disclosed by the service provider (e.g., third party audits and assessment, documentation of SAS70 Type II, ISO 17799/ISO 27001/ISO 27002, PCI DSS, BITS assessments, information security policies). The VSA team may also perform appropriate technical diagnostics, scanning and review of the service provider's infrastructure and services to identify any deficiencies or vulnerabilities.

The VSA team produces a written assessment of the service provider's information security

program and the service under review, including a description of the issues identified, the potential risks, recommendations for addressing the risks and a "can endorse" or "cannot endorse" rating. When the VSA team identifies deficiencies, service providers are asked to submit remediation plans. Google's VSA team also provides guidance on what contract clauses are needed with respect to the service provider. The service provider successfully completes this process when it has remediated any vulnerabilities that the VSA assessment identifies as posing a sufficiently substantial threat to the security or privacy of sensitive data or Google systems, implements a corrective action plan to address less significant vulnerabilities, obtains approval from Security Engineering, as appropriate, if the assessment identifies material residual risks, and accepts contract terms that maintain adequate protections for information security and privacy.

Standard Contractual Obligations

Google has adopted standard confidentiality contract provisions that require all service providers to provide appropriate protection for the confidentiality of any information received from Google, including covered information under the Order.

On November 4, 2011, Google added an additional control to its existing process by reassessing whether any service provider paid by Google through its purchase order requisition process has successfully completed Google's information due diligence and is subject to reasonable contractual obligations for the protection of user data. All Google requisition requests now require that Google staff indicate whether the service provider will receive information collected from or about Google users. All service providers who receive access to covered information are then reviewed by the Ethics and Compliance team to determine whether the VSA team has completed an assessment, whether the service provider has remediated vulnerabilities identified during the review, and is subject to appropriate privacy, confidentiality and security contract clauses.

In January 2012, Google revised the confidentiality obligations in its standard Purchase Order Terms and Conditions to require that Google service providers maintain "administrative, physical, and technical safeguards . . . that protect the security and privacy" of covered information, that "meet or exceed relevant industry standards" and are appropriate to the service provider's role, operations and exposure to covered information. In addition to the Terms and Conditions, Google negotiates a range of contracts with service providers, and the Ethics and Compliance team reviews and approves negotiated contracts to ensure that service providers are agreeing to appropriate privacy protections.

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.

Google's Privacy Effort regularly evaluates the results of testing and monitoring of privacy controls and adjusts the program accordingly to address identified risks. Many privacy controls, processes, and procedures exist throughout Google, (including, but not limited to, those described above in connection with Part III. C.,) with corresponding testing and monitoring mechanisms. The output of those mechanisms is used to focus resources and improve the performance and reliability of the overall Privacy Effort. Some of these outputs reflect, for example, changes in privacy risk resulting from material changes to Google's business operations or arrangements, or other circumstances that Google has reason to know may have a material impact on the effectiveness of its privacy program. One example of such reporting would be a PDD submission related to a new product feature which, when reviewed by the PWG and legal counsel, is determined to require the implementation of additional privacy controls to appropriately protect user privacy and satisfy applicable legal requirements. Cross functional teams including those dedicated to audit and compliance also engage in monitoring activities.

A specific example of control adjustment based on monitoring and review relates to the PDD review process. Through early monitoring the Privacy Working Group identified that additional communication and escalation may improve timely submission of PDDs. To accomplish this, Google implemented an automated reminder and escalation mechanism.

IV.

In connection with its compliance with part III of this order, respondent shall 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. A person qualified to prepare such Assessments shall have a minimum of three (3) years of experience in the field of privacy and data protection. All persons conducting such Assessments and preparing such reports shall be approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, DC 20580, in his or her sole discretion. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

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

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

C. explain how the privacy controls that have been implemented meet or exceed the protections required by Part III of this order; and

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.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent shall provide the initial Assessment to the Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, DC 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request.

Google has retained PriceWaterhouse Coopers LLP ("PWC") as its designated Assessor satisfying the requirements of this Part (pending approval from the Associate Director of Enforcement, in accordance with this Part).

V.

Respondent shall maintain and upon request make available to the Federal Trade Commission for inspection and copying, unless respondent asserts a valid legal privilege, a print or electronic copy of:

A. for a period of three (3) years from the date of preparation or dissemination, whichever is later, all widely disseminated statements that describe the extent to which respondent maintains and protects the privacy of any covered information, with all materials relied upon in making or disseminating such statements;

Google presently maintains such statements, and will make them available to the Commission upon request in accordance with the requirements of this Part.

B. for a period of six (6) months from the date received, all consumer complaints directed at respondent, or forwarded to respondent by a third party, that allege unauthorized collection, use, or disclosure of covered information and any responses to such complaints.

Google presently maintains such statements, and will make them available to the Commission upon request in accordance with the requirements of this Part.

C. for a period of five (5) years from the date received, any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent's compliance with this order;

Google shall retain and make all non-privileged responsive documents available to the FTC as required by this Part upon request.

and

D. for a period of three (3) years after the date of preparation of each Assessment required under Part III of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of respondent, including, but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, for the compliance period covered by such Assessment.

Google shall retain and make all non-privileged responsive documents available to the FTC as required by this Part upon request.

VI.

Respondent shall deliver a copy of this order to all current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having supervisory responsibilities relating to the subject matter of this order. Respondent shall deliver this order to such current personnel within thirty days after the service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities.

On November 23, 2011, Google timely distributed a copy of the Order via email to all current employees at manager level or above. The email message included an email address to which recipients could direct questions regarding the Order. On November 23, 2011, a separate email was distributed to each member of the Google Board of Directors, including an electronic copy of the Order.

On December 23 and January 23, 2011, a similar email was distributed to all new Google employees at manager level or above, as well as existing employees whom had been promoted to manager level since the prior distribution. A process has been established by

which the Order will be similarly distributed monthly to all new managers or other individuals with supervisory responsibilities relevant to Google's compliance with the Order.

VII.

Respondent shall notify the Commission at least thirty (30) days prior to any change in the corporation that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the filing of a bankruptcy petition; or a change in either corporate name or address. Provided, however, that, with respect to any proposed name change in the corporation about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. All notices required by this Part shall be sent by certified mail to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, DC 20580.

Google shall notify the Commission, in accordance with and as required by this Part, should any event triggering such requirement under this Part occur.

VIII.

Respondent shall, within ninety (90) days after the date of service of this order file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form in which respondent has complied with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, respondent shall submit additional true and accurate reports.

I affirm under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on January 26, 2012.

Keith Enright
Senior Privacy Counsel
Google Inc.