



**Independent Assessor's Transmittal Letter on
Google LLC's Privacy Program**

For the Period of April 26, 2016 to April 25, 2018

With Report of Independent Accountants

CONFIDENTIAL

Table of Contents

Transmittal Letter.....	1
EY's Privacy Assessment Approach	2
Independence	
EY Assessment Process Overview	
EY's Assessment of Part IV A – D of the Agreement Containing Consent Order File No.: 1023136 (the "Order")	6
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 have been implemented to meet or exceed the protections required by Part III of the Order	
D. Certify that the privacy controls are operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the reporting period	
Addendum to Transmittal Letter	12
Overview of Company.....	12
Company Overview	
EY's Review of Google's Privacy Program.....	12
Privacy Program review	
Google's privacy policies	
Privacy Program teams	
Google Privacy Program assessment	
Google's product launch privacy review process	
End-user privacy settings	
Privacy training and awareness programs	
Third party risk management	
EU/US Privacy Shield process	
Independent Assessor's Examination Report on Google LLC's Privacy Program	25



Report of Independent Accountants.....	26
Exhibit I: Management’s Assertion.....	28
Attachment A: Google’s Privacy Program Criteria, Supporting Controls, and Assessment Results	29
Attachment B: Assessment Interviews Summary.....	43



Ernst & Young LLP
303 Almaden Boulevard
San Jose, CA 95110

Tel : +1 408 947 5500
Fax: +1 408 947 5717
ey.com

Mr. Keith Enright
Director, Privacy Legal
Google LLC
345 Spear St.
San Francisco, CA 94105

Dear Mr. Enright,

We are issuing the attached Independent Assessor's Report on Google LLC's¹ ("Google" or "the Company") Privacy Program ("Report") in connection with our examination to determine whether for the two years ended April 25, 2018 (the "Reporting Period"), in accordance with Parts III and IV of the Agreement Containing Consent Order File No.: 1023136 (the "Order"), with a service date of October 28, 2011, between Google and the Federal Trade Commission ("FTC"):

- The Company established and implemented a comprehensive privacy program (the "Subject Matter" or "Privacy Program") based on the seven Google-specific statements ("Criteria") and supporting controls set forth in Attachment A;
- The Company's privacy controls are appropriate to its size and complexity, the nature and scope of its activities, and the sensitivity of covered information (as defined in the Order)²;
- The Company's privacy controls meet or exceed the protections required by Part III of the Order; and
- The Company's privacy controls are operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and have so operated throughout the Reporting Period.

This letter should be read in conjunction with the Report.

Part III of the Order requires Google to "establish and implement, and thereafter maintain, a comprehensive privacy program that is reasonably designed to: (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information. Such program, the content and implementation of which must be documented in writing, shall contain privacy controls and procedures appropriate to [Google's] size and complexity, the nature and scope of [Google's] activities, and the sensitivity of the covered information."

¹ Google Inc. became Google LLC during the Reporting Period.

² The Order defines "covered information" as "information that [Google] collects from or about an individual, including, but not limited to, an individual's: (a) first and last name; (b) home or other physical address, including street name and city or town; (c) email address or other online contact information, such as a user identifier or screen name; (d) persistent identifier, such as IP address; (e) telephone number, including home telephone number and mobile telephone number; (f) list of contacts; (g) physical location; or any other information from or about an individual consumer that is combined with (a) through (g) above."



Part IV of the Order requires Google to obtain biennial assessments (“Assessments”) of its Privacy Program from a “qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession.” Google retained Ernst & Young (“EY”) to perform the Assessment for the biennial period beginning April 26, 2016 and ending April 25, 2018 (“Reporting Period”). The Assessment covered Google LLC and its affiliates subject to this Order.

EY’s Privacy Assessment Approach

Part IV of the Order requires that the assessments be performed by “a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession.” This report was issued by EY under applicable professional standards that meet these requirements.

EY, an American Institute of Certified Public Accountants (“AICPA”) member firm, must comply with the public accounting profession’s technical and ethical standards, including the AICPA’s Code of Professional Conduct. In addition to the Code of Professional Conduct, the AICPA publishes standards, which delineate specific requirements Certified Public Accountants are consistently required to follow in the course of engagements.

One such standard, the Concepts Common to All Attestation Engagements (AT-C Section 105), states that practitioners must meet specific requirements to accept and perform assessments, such as the following:

Assignment of the Engagement Team and the Practitioner’s Specialists:

The engagement partner should be satisfied that:

- a. the engagement team, and any practitioner’s external specialists, collectively, must have the appropriate competence, including knowledge of the subject matter, and capabilities to
 - i. perform the engagement in accordance with professional standards and applicable legal and regulatory requirements and
 - ii. enable the issuance of a practitioner’s report that is appropriate in the circumstances.

Furthermore, “[t]he responsible party in an attestation engagement must have a reasonable basis for measuring or evaluating the subject matter.”

In performing this Assessment, EY complied with all these standards. Furthermore, all EY personnel directing the examination were sufficiently qualified. All EY personnel directing the examination and preparing the Report had a minimum of three years’ experience in the field of privacy and data protection.



Independence

AICPA standards also require EY to maintain independence in the performance of audit and examination engagements. The AICPA standard states, “[a] member in public practice shall be independent in the performance of professional services as required by standards promulgated by bodies designated by Council” (AICPA Code of Professional Conduct sec. 1.200 Independence). The standard states that to determine whether an auditor has the requisite independence in the performance of professional services, an AICPA “member should evaluate whether the relationship or circumstances would lead a reasonable and informed third party who is aware of the relevant information to conclude that there is a threat to either the member’s or the firm’s independence, or both, that is not at an acceptable level.”

Independence is comprised of independence of mind and independence in appearance, both of which are required of the AICPA member firm and the auditors engaged in the professional service. Independence of mind requires that the member maintain a state of mind that permits the expression of a conclusion without being affected by influences that compromise professional judgment, thereby allowing an individual to act with integrity and exercise objectivity and skepticism. Independence of appearance is achieved by the avoidance of facts and circumstances that are so significant that a reasonable and informed third party would likely conclude, weighing all the specific facts and circumstances, that a firm’s, or a member of the audit team’s, integrity, objectivity, or professional skepticism has been compromised.

EY is independent in accordance with the AICPA standards required for this engagement.

EY Assessment Process Overview

The procedures performed by EY were designed to:

- Examine Management’s Assertion concerning Google’s compliance with Part III of the Order, stating that Google has maintained the Google Privacy Program (“Subject Matter”) to meet the requirements of the Google FTC Order based on the Criteria and supporting controls;
- Examine the design effectiveness of the controls implemented by Google to address the Criteria; and
- Examine the operating effectiveness of the implemented controls during the Reporting Period.

EY performed procedures to evaluate the design and operating effectiveness of the controls implemented and/or maintained by Google during the Reporting Period. The nature of EY’s testing was dependent on each control, and EY developed a test procedure based on our understanding of the risk, complexity, extent of judgment, and other factors. EY used a combination of inquiry, observation, and inspection for testing of the controls. Refer below for a description of the test procedures utilized by EY:

Inquiry: To understand the design of the controls implemented by Google and how they operate to meet or exceed the protections required by the Order, EY held discussions with Google personnel to obtain an understanding of Google's overall Privacy Program and its objectives. Google personnel included individuals from various departments, a listing of which is included in *Attachment B: Assessment Interviews Summary*. The inquiry procedures included asking the Google personnel about the controls, policies, and procedures, as well as their roles and responsibilities. To validate the information obtained in the discussions, EY performed corroborative inquiry procedures with multiple individuals and, using the testing techniques below, obtained additional evidence to validate the responses. When EY performed corroborative inquiry, EY asked several people across Google about a given control or situation. EY does not rely on inquiry procedures alone, but rather, combines inquiry procedures with additional forms of testing (i.e., observation or inspection/examination) to evaluate and reach conclusions on the effectiveness of the controls.

Observation: EY utilized the observation testing method to validate the design and operating effectiveness of the controls. To determine whether Google has implemented controls that meet or exceed the Criteria on which Management's Assertion is based, EY met with relevant Google personnel and observed how the controls were designed and how they functioned.

Examination or inspection of evidence: EY used the examination or inspection test approach to validate the operating effectiveness of the controls and to evaluate the sufficiency of the controls implemented to meet or exceed the Criteria on which Management's Assertion is based. EY inspected, physically or online, artifacts and documents (including documentation of Google's policies and procedures, risk assessment, and training and awareness programs) to evidence the design and operating effectiveness of the controls and safeguards implemented by Google. The nature of the evidence examined varied from control to control and, where appropriate, other procedures like observation and inquiry were utilized to confirm the results of the examination procedures.

To assess design effectiveness, EY performed walkthroughs of the processes and controls to determine whether the controls were built to achieve the Criteria on which Management's Assertion is based, as well as to determine whether the controls had been placed into operation. To perform a walkthrough, EY met with relevant Google control owners and interviewed them on how Google implemented the controls. Additionally, during the design assessment, EY assessed whether the individuals performing the controls possessed the necessary authority and competence to perform the controls effectively. Our design effectiveness test procedures included performing a combination of inquiry, observation, inspection, and examination.

To assess operating effectiveness, EY performed procedures to determine whether the controls were executed by Google (or Google's systems, if automated) on a regular frequency, and whether documentation and support were maintained to evidence the controls' execution. Our operating effectiveness test procedures included, where appropriate, selecting samples from the



populations representing the Reporting Period and performing a combination of inquiry, observation, and/or inspection/examination procedures to evaluate the effectiveness of the controls documented in *Attachment A: Google's Privacy Program Criteria, Supporting Controls, Test Procedures, and Assessment Results*.

Over the course of the Reporting Period, EY performed procedures that included interviewing individuals from the Privacy and Data Protection Office, Privacy Legal, Ethics & Compliance, Information Security, Engineering Compliance, Privacy Engineering, Detection & Response, Internal Audit, Security and Privacy Mergers & Acquisitions, Product Management, and Security & Privacy EDU. Please see *Attachment B: Assessment Interviews Summary* for individuals interviewed as a part of the Assessment. Please see *Addendum to Transmittal Letter* for more information on EY's review of Google's privacy program.

Please let us know if you have any questions. [REDACTED]

Ernst & Young LLP

June 25, 2018
San Jose, California



EY's Assessment of Part IV A – D of the Agreement Containing Consent Order File No.: 1023136 (the "Order")

Attachment A: Google's Privacy Program Criteria, Supporting Controls, Test Procedures, and Assessment Results sets forth tables that describe the scope of Google's Privacy Program subject to this Assessment. Google established its Privacy Program by implementing privacy controls to meet or exceed the protections required by Part III of the Order. The section below documents EY's assessment results. EY's final conclusions on Management's Assertion are detailed in the Report.

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

As depicted within *Attachment A: Google's Privacy Program Criteria, Supporting Controls, Test Procedures, and Assessment Results*, Google has listed the controls that were implemented and maintained during the Reporting Period. Our procedures, as defined in the section entitled, "EY Assessment Process Overview," support the results of our assessment that the controls have been implemented and maintained during the Reporting Period.

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

Based on the size and complexity of the organization, the nature and scope of Google's activities, and the sensitivity of the covered information, Google's management developed the Criteria and supporting controls detailed in *Attachment A: Google's Privacy Program Criteria, Supporting Controls, Test Procedures, and Assessment Results* as the basis for its Privacy Program. Those Criteria and supporting controls are intended to address the risks identified by Google's privacy risk assessment. The Criteria and supporting controls were evaluated against the AICPA standards for suitable and available criteria (AT-C 105, .A42), which requires criteria to be:

- (1) Relevant to the subject matter;
- (2) Objective and free from bias;
- (3) Consistently measurable using qualitative or quantitative attributes; and
- (4) Complete and not missing any factors that could reasonably be expected to affect decisions of the intended users made on the basis of that subject matter.

Upon evaluation of the Criteria, EY confirmed that the Criteria were relevant, objective, measurable, and complete to address the risks identified by Google's privacy risk assessment in each of the areas defined by Management's Assertion, therefore the Criteria are appropriate to Google's size and complexity, the nature and scope of Google's activities, and the sensitivity of Google's covered information.



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

As summarized in *Attachment A: Google's Privacy Program Criteria, Supporting Controls, Test Procedures, and Assessment Results*, Google has implemented the following protections:

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

Google implemented the following controls in order to meet this requirement:

2.1	Privacy roles and responsibilities of employees and groups that play a part in privacy at Google are defined and published.
2.2	Google maintains an online privacy organizational chart and communication model.
2.3	A working group of privacy subject matter experts provides oversight of privacy topics at Google.

As described above, Google has designated a team of employees to coordinate and share responsibility for the Privacy Program. EY performed test procedures to assess the effectiveness of Google's privacy controls to meet or exceed the protections required by Part III of the Order.

B. The identification of reasonably foreseeable, material risks, both internal and external, that could result in respondent's unauthorized collection, use, or disclosure of Covered Information, and an assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this privacy risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management, including training on the requirements of this Order, and (2) product design, development, and research.

Google implemented the following controls to meet this requirement:

3.1 (7.1)	Google Privacy Teams conduct periodic risk assessments to: <ul style="list-style-type: none">• Identify external and internal risks;• Assess existing privacy controls;• Assess risks in product design, development, and research;• Consider changes in the regulatory environment; and• Consider the impact of any changes to Google operations or business arrangements (e.g., acquisitions, divestitures).
3.2 (7.2)	Google Privacy Teams review the Risk Assessment results and identify opportunities to further reduce and mitigate risks.
3.3	Risk Assessment results are communicated to privacy leadership in a timely manner.

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. EY performed test procedures to assess the effectiveness of Google's privacy controls to meet or exceed the protections required by Part III of the Order.

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 the privacy controls and procedures.

Google implemented the following controls to meet this requirement:

4.1	Google's privacy design documentation is required to be completed, and privacy design is reviewed prior to product launch.
4.2	Google facilitates transparency and choice by providing end-user privacy settings, which include: <ul style="list-style-type: none"> • Account management tools (e.g., My Account, Dashboard, Activity Controls, Account Permissions for Connected Apps and Sites, Inactive Account Manager, Account and Service Deletion); • Product settings (e.g., Ads Settings, Google+/Social Settings, Search Personalization Settings, Analytics Opt-Out); • Privacy tools and guides (e.g., Privacy Checkup, Product Privacy Guide, Incognito Mode); • Security tools and guides (e.g., Security Checkup, 2-Step Verification, Device Activity and Notifications, Service Encryption, Chrome Safe Browsing); • Tools for exporting user data from Google products (e.g., Takeout); and • Google Transparency Report.
4.3	Google privacy engineers perform privacy code audits, and results are reviewed by stakeholders.
4.4	Google privacy teams provide supplemental training and awareness programs including a privacy awareness week, privacy workshops, and advanced privacy training courses.
4.5	Google employees are required to complete training about Google privacy policies and practices within 90 days of hire date and at least biennially thereafter, and completion is followed-up on by management.
4.6	Foundational privacy training is required of new Google engineers, and completion is followed-up on by management.
4.7	Google has established feedback processes that give internal users the ability to voice privacy concerns, which are monitored.
4.8	Google has established feedback processes that give external users the ability to voice privacy concerns, which are monitored.

4.9	Google has an incident response program in place with established processes for responding to privacy incidents. The program and its processes are documented and reviewed periodically. Privacy incidents are monitored and tracked in accordance with internal policy.
4.10	On an annual basis, Google Product Managers and Tech Leads attest to the accuracy, comprehensiveness, and implementation of the applicable privacy policies or that they have identified any changes that need to be made to reflect current practices.
4.11	Google has an entity wide information security program that supports the Google Privacy Program. Google engages third parties throughout the year to perform assessments of its security program.
4.12	Google employees are required to sign a code of conduct acknowledgement upon employment.
4.13	Google employees are required to sign confidentiality agreements upon employment.
4.14	Google maintains sites containing applicable external privacy policies and supplemental reference materials explaining those policies.
5.1	Privacy is considered and documented as part of scoping and execution (where applicable) for internal audits at Google.
5.2 (7.3)	Internal Audit performs a periodic assessment of key Google privacy controls. Results are shared with Google privacy teams and other stakeholders as necessary and are considered for ongoing improvement of the privacy program.
5.3	Privacy leadership periodically reviews internal reports on the functioning of the privacy review process.
5.4	Google management reviews and confirms the completion of the Privacy Shield process for Google.

EY evaluated the processes and controls Google placed in operation to address risks Management may have identified in their risk assessment. As described above, Google has designed and implemented reasonable controls and procedures to address the risks identified through the privacy risk assessment, and regular testing or monitoring of the effectiveness of those controls and procedures. EY performed test procedures to assess the design and operating effectiveness of Google's privacy controls to meet or exceed the protections required by Part III of the Order.

D. The development and use of reasonable steps to select and retain service providers capable of maintaining security practices consistent with this order, and requiring service providers by contract to implement and maintain appropriate safeguards.

Google implemented the following controls to meet this requirement:

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

6.2	Google service providers are required to sign confidentiality terms as part of the agreement, as deemed necessary.
6.3	Google teams review Google service providers using a risk-based assessment process.

As described above, Google has developed and implemented reasonable steps to select and retain service providers capable of maintaining security practices consistent with the Order, and requiring service providers by contract to implement and maintain appropriate safeguards over covered information they receive from Google. Google also includes terms in contracts with service providers requiring that such service providers implement and maintain appropriate privacy protections. EY performed test procedures to assess the design and operating effectiveness of Google's privacy controls to meet or exceed the protections required by Part III of the Order.

E. The evaluation and adjustment of respondent's privacy program in light of the results of the testing and monitoring required by subpart C, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its privacy program.

Google implemented the following controls to meet this requirement:

7.1 (3.1)	Google privacy teams conduct periodic risk assessments to: <ul style="list-style-type: none"> • Identify external and internal risks; • Assess existing privacy controls; • Assess risks in product design, development, and research; • Consider changes in the regulatory environment; and • Consider the impact of any changes to Google operations or business arrangements (e.g., acquisitions, divestitures).
7.2 (3.2)	Google privacy teams review the Risk Assessment results and identify opportunities to further reduce or mitigate risk.
7.3 (5.2)	Internal Audit performs a periodic assessment of key Google privacy controls. Results are shared with Google privacy teams and other stakeholders as necessary and are considered for ongoing improvement of the privacy program.
7.4	Findings and recommendations that come as a result of Internal Audit testing of the Google Privacy Program are communicated to privacy leadership as applicable.
7.5	Action items identified from the results of Internal Audit control testing of the Google Privacy Program are assigned an owner and tracked to ensure remediation.

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 Part III of the Order, 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. EY performed test procedures to assess the effectiveness of Google's privacy controls to meet or exceed the protections required by Part III of the Order.

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

As described in the EY Assessment section above, EY performed its assessment of Google's Privacy Program in accordance with AICPA Attestation Standards. Refer to the Report for EY's opinion, which provides the conclusion of our assessment.

Addendum to Transmittal Letter

Overview of Company

Company overview

Google is a global technology service provider focused on organizing the world's information to make it universally accessible and useful.³ This lists just a few of Google's wide-ranging products:

- Search;
- AdWords;
- Gmail;
- Google Maps;
- Google Apps, including Google Docs, Google Sheets, and Google Drive;
- Blogger;
- Google Chrome;
- Android;
- Google Pay;
- YouTube; and
- Google Home.

Google became a publicly traded company on August 18, 2004. The Company now has offices in more than 40 countries and provides products and services in over 130 languages to Google users all over the world. It is headquartered in Mountain View, California and employs more than 75,000 people. Google is a wholly owned subsidiary of Alphabet Inc.

EY's Review of Google's Privacy Program

Privacy Program review

Over the course of the examination, through discussions with key individuals and observation of related documentation, EY reviewed the following aspects of Google's Privacy Program:

- Google's privacy policies
- Privacy Program teams
- Google's Privacy Program assessment
- Google's product launch privacy review process
- End-user privacy settings
- Privacy training and awareness programs
- Incident response program
- Third party risk management
- EU/US Privacy Shield process

³ Google Mission Statement, <https://www.google.com/about/our-company/>

The following section describes highlights of each component, which support the overall Privacy Program.

Google's privacy policies

The Google Privacy Program is documented in several internal policies, and supplemented by guidance documents. The policies and guidance documents are accessible from Google's intranet by all employees of the Company. The internal policies cover core requirements under Google's Privacy Program, including:

- Privacy training requirements
- Classification and handling of anonymous data
- Use of cookies and other client-side management mechanisms on Google products
- Rules of exporting user data
- Rules for collecting, accessing, processing, and handling user data
- Retention and deletion requirements around user data
- Requirements for reporting and responding to potential privacy incidents
- Principles for providing additional notice and obtaining additional consent
- Rules for the use of immutable identifiers in Google products

EY noted that the policies had been reviewed and updated during the Reporting Period.

Google's public-facing privacy policy describes to users what information Google collects from users, the sources from which Google obtains this information, and how the collected information is used. The policy has a section called "transparency and choice," which describes various controls a user has about how their information is collected, used, and presented to others. A screenshot of this privacy policy, reviewed during the examination and available publicly, is shown below.⁴

⁴ The public-facing privacy policy from the Reporting Period can be found here:
https://static.googleusercontent.com/media/www.google.com/en/intl/en/policies/privacy/google_privacy_policy_en.pdf



Privacy Policy

Last modified: December 18, 2017 ([view archived versions](#)) (The hyperlinked examples are available at the end of this document.)

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](#).

Privacy Program teams

The Google Privacy Program is operated by a cross-functional team of employees representing:

- Privacy Working Groups (PWG)
- Privacy Legal
- Privacy & Data Protection
- Ethics & Compliance
- Security
- Privacy Engineering
- Incident Detection & Response
- Internal Audit
- Security and Privacy Mergers & Acquisitions
- Security & Privacy EDU
- Product Management

Privacy Working Groups (PWG) are composed of privacy subject matter experts, providing advice on privacy issues and overseeing the privacy review process related to the Privacy Program. Privacy working groups are established for various privacy topics and for various product areas, such as YouTube and Hangouts. Any Google employee who has a privacy question can reach out directly to a PWG member, or send a message to a general PWG inbox to obtain guidance

and instructions on how to address the issue in line with Google's privacy policies. PWG members escalate privacy issues and concerns as necessary to privacy leadership.

In addition to the Google teams that are focused on privacy, individuals within departments throughout the organization are tasked with certain privacy responsibilities. For example, within the Legal Department, hundreds of Product Counsel are responsible for assisting product teams with privacy reviews related to product launches. Product Counsel are also tasked with completing Privacy Shield reviews and attestations for their respective products.

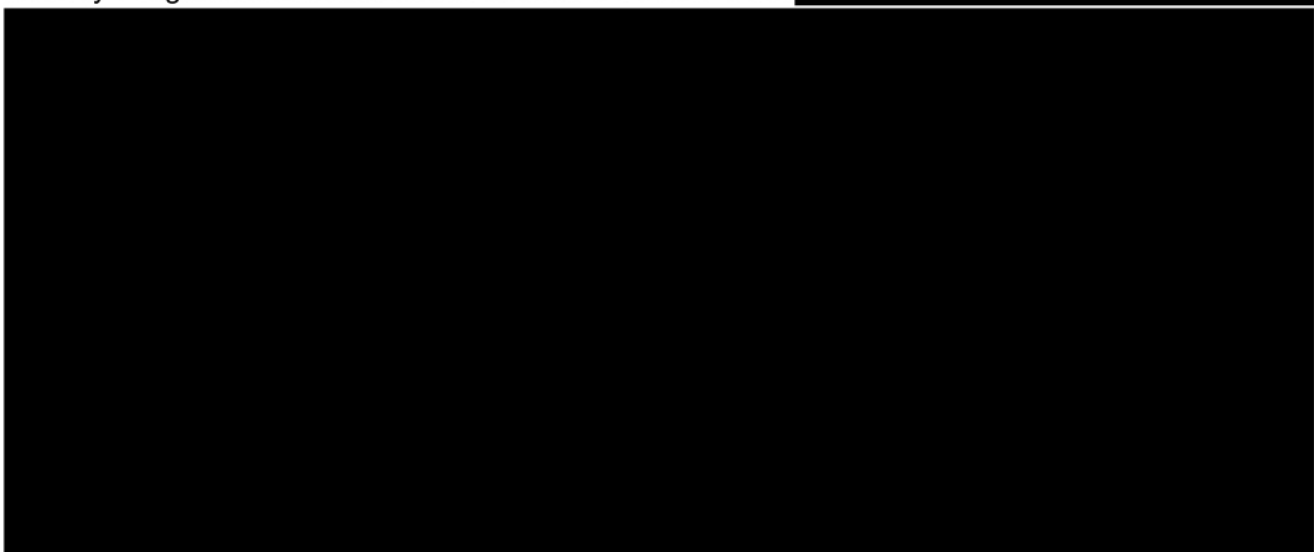
Google Privacy Program assessment

In anticipation of, and to adapt to changes in the business and regulatory landscape, Google periodically reviews its Privacy Program. The Google Privacy Program is reviewed in five ways: (1) periodic meetings between key privacy program leadership members, (2) periodic all-hands meetings to discuss privacy issues and topics and to field questions from employees, (3) biennial independent third-party assessments required under this Order, (4) biennial internal audits of the Google Privacy Program, and (5) annual risk assessments.

In addition to helping identify privacy program changes, the annual risk assessment is designed to achieve the following objectives:

- Identify external and internal risks;
- Assess existing privacy controls;
- Assess risks in product design, development, and research;
- Consider changes in the regulatory environment; and
- Consider the impact of any changes to Google operations or business arrangements (e.g., acquisitions, divestitures).

The Google privacy team evaluates the evolving risk landscape and the ability of the Google Privacy Program's current controls to address those risks. [REDACTED]



The existing privacy controls are mapped to the identified risks and, where there are instances of newly discovered risks that are not adequately managed by current controls, additional controls are developed, added to the Privacy Program, and included in the scope of future audits.

Google's product launch privacy review process

Google requires all product teams to complete a Privacy Design Document (PDD) prior to launch of all products that Google defines as privacy-impacting. The PDD is an example of how Google integrates privacy by design within their products. Each PDD contains information pertaining to the nature of the product being developed, the type of data that it will collect, how the data will be used, who it will be shared with, and the controls (privacy, security, or other related controls) that will be implemented to protect that data. PDDs are reviewed by a privacy reviewer prior to a product being approved for launch.

The PDD template evolves depending on the needs of the product, company, or changes to the Privacy Program. For example, during the course of EY's assessment, enhancements were made to the PDD template to reflect the requirements of the General Data Protection Regulation (GDPR).

End-user privacy settings

Google provides users with transparency and choice into Google application privacy settings through the My Account feature. My Account provides a centralized location where users are able to exercise control over aspects of how a user's data is handled by Google. My Account includes two walkthroughs for users: Privacy Checkup and Security Checkup. Each checkup asks the user a series of questions about a user's preferences regarding privacy or security, respectively. Some of the choices provided to the user include:

- Managing account activity-based ads personalization;
- Deleting account activity (including browser activity);
- Managing voice and audio for vocal commands;
- Managing YouTube watch and search history
- Managing geolocation; and
- Managing whether activities are publicly visible on Google products

A screenshot of the My Account feature, which can be accessed from all Google accounts, is provided below⁵.

⁵ https://myaccount.google.com/?utm_source=OGB&utm_medium=app



Welcome, [redacted]

Control, protect, and secure your account, all in one place

Your Google Account gives you quick access to settings and tools that let you safeguard your data, protect your privacy, and decide how your information can make Google services work better for you.

Sign-in & security >

Control your password and Google Account access.

[Signing in to Google](#)

[Device activity & security events](#)

[Apps with account access](#)



Security Checkup

Protect your account in just a few minutes by reviewing your security settings and activity

[GET STARTED](#)



Find your phone

Whether you forgot where you left it or it was stolen, a few steps may help secure your phone or tablet

[GET STARTED](#)

Personal info & privacy >

Manage your visibility settings and the data we use to personalize your experience.

[Your personal info](#)

[Contacts](#)

[Manage your Google activity](#)

[Ads Settings](#)

[Control your content](#)



Privacy Checkup

Take this quick checkup to review important privacy settings and adjust them to your preference

[GET STARTED](#)



My Activity

Discover and control the data that's created when you use Google services

[GO TO MY ACTIVITY](#)

Account preferences >

Adjust account settings, like payment methods, languages, & storage options.

[Payments](#)

[Purchases, subscriptions & reservations](#)

[Language & Input Tools](#)

[Accessibility](#)

[Your Google Drive storage](#)

[Delete your account or services](#)



We're committed to your privacy and security.

[LEARN MORE](#)

The My Account feature contains the following privacy-related setting and tool options:

TYPE	NAME	DESCRIPTION
Sign-in & security	Signing into Google	Provides users with the ability to update their password, turn on two-step verification, and choose account recovery options
	Device activity & security events	Lists recent security events on the user's account and shows devices recently used to access the user's account
	Apps with account access	Allows the user to keep track of which apps and services the user has given permission to access his/her Google account, and shows what apps and sites Google Smart Lock has saved passwords for
	Security Checkup	At-a-glance review of any security issues detected on the user's account. Shows the user's devices, recent security activity, methods of sign-in and recovery verification, and third parties that have access to the user's data
	Find your phone	Assists the user in finding any mobile or tablet devices that can be used to access the user's account

TYPE	NAME	DESCRIPTION
Personal info & privacy	Your personal info	Allows user to manage basic personal information (including name, phone number, and email) stored about the user. Also allows the user to update different privacy settings.
	Contacts	Allows the user to manage contact settings, including automatically saving contact info from interactions and allowing the user to block unwanted contacts
	Manage your Google activity	Allows the user to choose what activity data is saved to create the user's customized Google experience. Provides a link to Dashboard, which organizes the user's data by product and shows the user Google services the user has shared data with

TYPE	NAME	DESCRIPTION
	Ads Settings	Allows the user to choose how Google uses the user's Google Account activity to personalize ads shown to the user. Notifies the user that Google does not share personally identifiable information about the user with Google's partners. Allows the user to choose topics the user likes and would prefer to see ads about
	Control your content	Allows the user to create an archive of the user's content from Google products. Allows the user to assign an account trustee in the event the user's account has been left unattended for an amount of time specified by the user
	Privacy Checkup	Walks the user through privacy choices across Google products, including whether Google saves location history, whether the user's device will respond to audio commands to turn on Google (such as "Ok, Google"), and whether the user's YouTube watch history is saved
	My Activity	Allows a user to review saved Google activity across platforms and delete specific activities manually, or delete activities based on dates or products on which the activities were performed

Google also provides the user with the ability to export his/her data from any Google products using Google Takeout, displayed below⁶.

← Download your data

Your account, your data.
Export a copy.

Create an archive with your data from Google products.

MANAGE ARCHIVES

Select data to include

Choose the Google products to include in your archive and configure the settings for each product. This archive will only be accessible to you. [Learn more](#)

Product	Details		SELECT NONE
+1s		▼ <input checked="" type="checkbox"/>	
Android Device Configuration Service		▼ <input checked="" type="checkbox"/>	
Blogger		▼ <input checked="" type="checkbox"/>	
Bookmarks		▼ <input checked="" type="checkbox"/>	
Calendar	All calendars	▼ <input checked="" type="checkbox"/>	
Chrome	All Chrome data types	▼ <input checked="" type="checkbox"/>	
Classroom		<input checked="" type="checkbox"/>	
Cloud Print		<input checked="" type="checkbox"/>	

⁶ The Google Takeout webpage can be found at: <https://takeout.google.com/?pli=1>

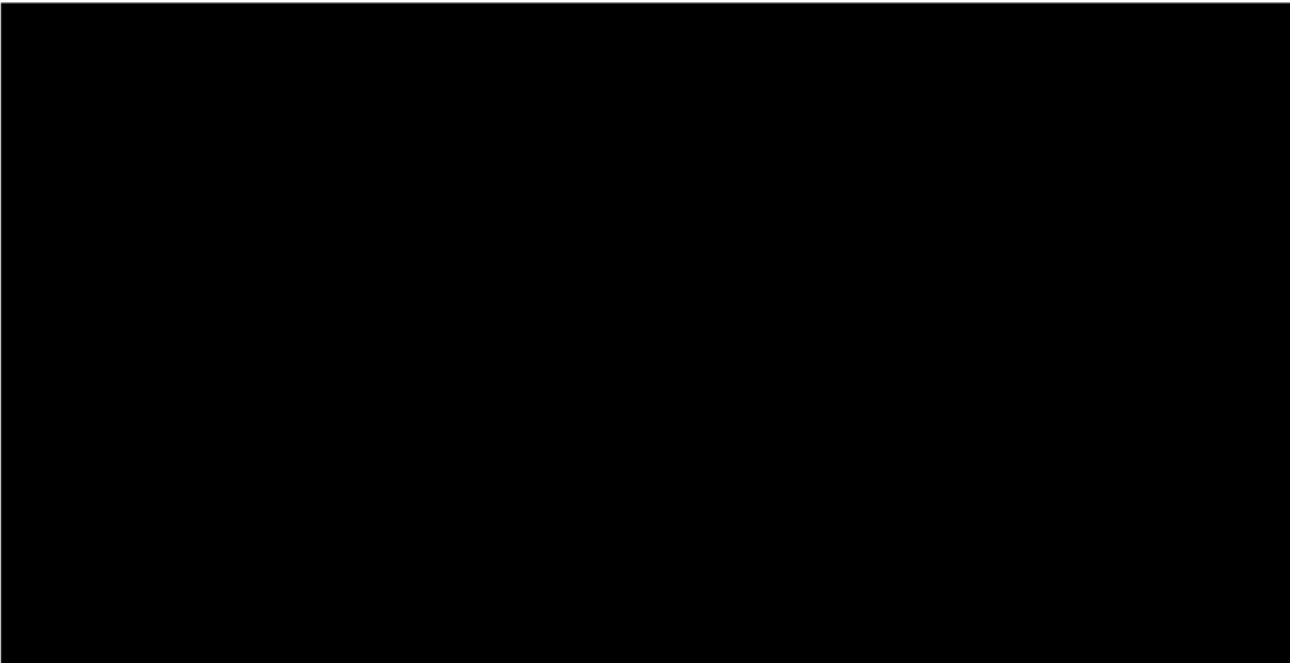
Privacy training and awareness programs

Google requires all new hires to complete privacy training within 90 days of hire, and biennially thereafter. The privacy training consists of scenarios that challenge the employee to consider situations applicable to the employee's role and determine what course of action is most appropriate under Google's Privacy Policy and Google's Privacy Principles. As visible on Google's publicly available website, <https://policies.google.com/technologies>, Google's Privacy Principles "help guide decisions [Google employees] make at every level of [the] company." Google's Privacy Principles are displayed in the graphic below, observed by EY during the examination:



These Principles are embedded in the privacy training. Completion of training is tracked and management follows up with employees as necessary.

In addition to the basic privacy training, new engineers are required to complete engineer-specific privacy training upon hire. The new engineer training sets the tone for how Google expects engineers to treat user data. The new engineer training is structured against the Privacy Principles, described above, and provides examples of each principle in practice, using a situation that is relatable to the engineer. An excerpt from the engineering training course, Privacy Principles in Practice, under "Privacy Principle 4. Give users meaningful choices to protect privacy," which EY observed during the examination, is shown below.



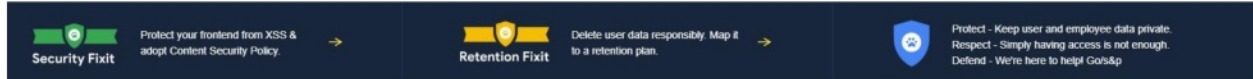
There are also a series of other supplemental trainings available to Google employees both within the Google training module, and also through the “Privacy and Security Week” (as held in 2016) and “Security and Privacy Month” (as held in 2017, and anticipated going forward). This Privacy and Security programming is available to all Google employees, worldwide. The event is publicized through newsletters, emails, office decorations, and branded swag distributed throughout the offices. The 2016 Privacy and Security Week consisted of 26 events, including trainings, talks, and privacy “hack-a-thons.” The 2017 Security and Privacy Month expanded this to 50 events, as well as a dedicated landing page for the programming, where users could register for the sessions. A screenshot of the internal website for the 2017 Security and Privacy Month, which EY observed during the examination, is shown below.

PROTECT RESPECT DEFEND!



Security & Privacy Month

October 2017 • go/spm17



Incident response program

For any privacy or security suspected incident, an employee is required to report the incident, which may be done through various channels such as through the dedicated email alias, phone number, or digital platform. For each suspected incident, a coordinated team is assigned to manage the overall incident, as well as liaising with Legal and the product team as part of the investigation and response. The team on-call for an incident is predetermined, based on a daily rotation. Incident responses may follow either a standard or expedited route, depending on the severity and priority assigned to the incident.

Third party risk management

Google requires that a privacy and security assessment be completed for any engagement involving the disclosure of user, customer, or employee personal data to a third party. Googlers initiating the engagement are required to comply with Google's third party assessment process. This may involve [REDACTED]

[REDACTED] To support the requester (Google employee) in completing the assessment, Google maintains policies, guidelines, tools, and workflow management systems to assist the requester in this process. Where the requester answers affirmatively that data will be shared with the vendor, the assessment is reviewed by Google's Ethics & Compliance Third Party Data Protection Team to determine whether a Vendor Security Assessment (VSA) is required.

A dashboard with resources on third party management for Googlers, which EY observed during the Assessment, is shown below.



Ethics & Compliance Data Protection Third Parties



GOOGLER RESOURCES



LEGAL TEAM MEMBER RESOURCES



OFFICE HOURS



IPA WIZARD



EXCEPTIONS/ESCALATIONS (TBD)



TRAINING

PRIVACY SHIELD VENDOR LIST

EU/US Privacy Shield process

Each product in scope for Privacy Shield certification is required to go through an annual Privacy Shield review process, in which Product Managers and Tech Leads attest to compliance with the Privacy Shield Principles. The attestation for the certification consists of two parts: one part to be completed by the Product Manager and/or Tech Lead, and the other to be completed by Product Counsel. Prior to completing the attestations, the Product Manager and/or Tech Lead and the Product Counsel meet to go through the Privacy Shield requirements and review the product's privacy documentation.