



December 21, 2007

The Honorable Joe Barton
Ranking Member
United States House of Representatives
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515

Dear Congressman Barton:

Thank you for your letter of December 12, and for your questions about our privacy practices. We welcome your efforts to learn more about the privacy protections that we offer our users and the practices of the industry generally. We also were pleased to host your staff on Wednesday and Thursday at our Mountain View headquarters where they met with some of our most knowledgeable engineers and product managers, and with our privacy experts. We hope that these meetings provided valuable information about Google's commitment to privacy.

As you know, Google operates in a business landscape that is marked by rapid change, product innovation, and significant competition. Our services enable a broad range of expression and commerce, from the success of small businesses using our AdWords service to greater civic engagement through our Public Sector Initiative, which helps government put public information online. As we described to your staff, Google offers many innovative products and every new product has the central focus of satisfying our users.

We believe user trust is essential to building the best possible products. With every Google product, we work hard to earn and keep that trust with a long-standing commitment to protect the privacy of our users' personal information. At the bedrock of our privacy practices are three design fundamentals:

- **Transparency:** We believe in being upfront with our users about what information we collect and how we use it so that they can make informed choices about their personal information. We have been an industry leader in finding new ways to educate users about privacy, such as our Google Privacy Channel on YouTube (which you can find at www.youtube.com/googleprivacy) where we feature privacy videos that explain our privacy policies in simple, plain English.
- **Choice:** We strive to design our products in a way that gives users meaningful choices about how they use our services and what information they provide to us. Many of our products, such as our Search services, do not require users to provide any personally identifying

information at all. When we do ask for personal information, we also endeavor to provide features that give users control over that information. For example, our Google Talk instant messaging service includes an “off the record” feature that prevents either party from storing the chat.

- **Security:** We take seriously the protection of the data that our users entrust with us. Google employs some of the world’s best engineers in software and network security and has teams dedicated to developing and implementing policies, practices and technologies to protect this information.

Innovation is a critical part of our approach to privacy. To best innovate in privacy, we take the feedback of privacy advocates, government experts, our users, and other stakeholders. For example, we participated actively in the Federal Trade Commission’s November Town Hall on privacy and behavioral advertising. Over the course of two days, the Town Hall examined the online advertising marketplace and how consumer privacy may be implicated by various industry practices including behavioral targeting. Google, other companies engaged in online advertising, privacy groups, regulators, and other stakeholders participated in that event, and it’s our belief that the Town Hall was a significant step forward in developing industry-wide solutions to consumer privacy issues in online advertising.

On the public policy front, Google supports the creation of a federal privacy law that would accomplish several goals such as building consumer trust and protections; creating a uniform framework for privacy, which would create consistent levels of privacy from one jurisdiction to another; and putting penalties in place to punish and dissuade bad actors. We also work actively to help industry establish and improve self-regulating mechanisms, and we support efforts to help develop industry-wide privacy standards. For example, earlier this week, the FTC announced proposed industry standards for behavioral advertising, and we are studying this proposal carefully with the goal of being an active participant in the FTC’s process.

We certainly welcome the opportunity to work together with you and other interested lawmakers on efforts to enact a uniform federal privacy law, as well as your support of industry efforts to establish robust self-regulatory mechanisms for protecting consumers’ privacy.

We have attached to this letter the questions that you submitted to us in your letter of December 12 (in bold and italics), in each case followed by our answer to the question. We are pleased to answer your questions, and we believe that they are best understood in the context of broader industry practices, as are many issues relating to online privacy.

Concerns about online privacy cannot be solved by one company alone. Moreover, both technologies and best practices for protecting privacy are changing rapidly. We therefore encourage you and your staff to ask these questions of other providers of online services, and draw any conclusions you may reach from that broader context.

Letter to Congressman Barton

December 21, 2007

Page 3

We trust that you and your staff will find our answers informative and helpful to you as you continue to engage with us and other providers of online services, and we wish you a happy holiday season.

Sincerely,

A handwritten signature in black ink, appearing to read "Alan Davidson". The signature is fluid and cursive, with a long horizontal stroke extending to the right.

Alan Davidson
*Senior Policy Counsel and
Head of U.S. Public Policy
Google Inc.*

attachment

Attachment

Google Responses to Questions from Congressman Joe Barton

1. Please describe Google's retention policy with respect to the following data. Include in your response a description of the type of data retained (for example, URL, Internet Protocol [IP] address, date, time of connectivity); the length of time the data is retained; where the data is retained; who has access to the retained data; and how the data is removed, deleted, or anonymized once the retention period lapses.

Our data retention policies vary based on the type of service in question. Some of our services can be used without registration; that is, the user does not need to log in or authenticate to access and use the service. Our flagship search engine is a good example of this type of unauthenticated use. Any user can visit the Google web site from any computer and use our search engine without providing Personally Identifying Information (PII). For these services, Google retains very little data, typically just standard server log information which includes: the uniform resource locator (URL); the Internet Protocol (IP) address associated with the computer or proxy server from which the request originated; the time and date of the request; the operating system that runs on the computer; and the type of browser that runs on the computer. We also may collect a unique cookie ID generated for the computer from which the request originated.

We recently announced our plans to further anonymize this "unauthenticated" data after 18 months. Specifically, we will obfuscate both the IP address and the cookie, which, in some cases, can be used in association with other information to identify an individual. Further discussion of our anonymization plan is below and you can also read the March 2007 announcement of the policy on our blog at <http://googleblog.blogspot.com/2007/03/taking-steps-to-further-improve-our.html>.

There are other services, such as Gmail, Google Web History and Google Calendar, which are private and/or customized for the individual user. These customized services require registration (typically just a user name, alternate email address and country) in order to secure the account for that user. As a general matter, we try to retain this data for as long as the user wants it retained. Indeed, we build in features that allow users to control both the collection and deletion of their personal information.

In regards to the protection of this information, and for each of the services specifically discussed below, Google has software and network security teams dedicated to the protection of data and systems. We take appropriate security measures to protect against unauthorized access to or unauthorized alteration, disclosure or destruction of data. These include internal reviews of our data collection, storage and processing practices and security measures, as well as physical security measures to guard against unauthorized access to systems where we store personal data. We restrict access to personal information to Google employees, contractors and agents who need to know that information in order to operate, develop or improve our services. These individuals are bound by confidentiality obligations and may be subject to discipline, including termination and criminal prosecution, if they fail to meet these obligations.

Google's Privacy Policy governing our consumer services, including the services discussed below, can be found at www.google.com/privacy.html.

We address below individually each of the services you raise in your questions.

a. *Search queries on Google search;*

Our flagship search engine can be used without registering or providing any PII. When an unauthenticated user searches for the term “car,” we collect typical log data, such as the URL, including the search query; the IP address associated with the computer or proxy server from which the query originated; the time and date of the search; the operating system that runs on the computer; the type of browser that runs on the computer. We also may collect a unique cookie ID generated for the computer from which the query originated. The cookie is used to recognize the user preferences (*e.g.*, selected language interface, search results formats, etc.), but users may choose to delete the cookie from their browser and still use the service.

A description of this search log information is included in our Privacy Policy FAQs at www.google.com/privacy_faq.html. In addition, we have a video, “Google Search Privacy: Plain and Simple,” describing the server logs on our Google Privacy Channel here: <http://www.youtube.com/watch?v=kLgJYBRzUXY&feature=PlayList&p=ECB20E29232BCBBA&index=0>.

As announced last March, Google will anonymize the cookie ID and the last octet (typically one to three digits) of the IP address associated with search queries after 18 months. Even though neither an IP address nor a unique cookie ID is PII, we believe that our users would prefer that we further anonymize this data after a reasonable period of time. We plan to begin anonymizing our search logs in the manner described above beginning in January 2008.

Users also have the option of accessing our search services (including Google Maps, News and Images) when they are logged in as a registered user. If a user is logged into his or her Google Account, then the searches also may be recorded in association with that account. As described in more detail below, this record is fully transparent to the user, and the user has the ability to pause this function or delete any record.

b. *Search queries on Google maps;*

In addition to the actual query (*e.g.*, driving directions or a business location search query), we collect standard log information in Google Maps as that described above when a user enters a query on Google Search. We will handle search queries on Google Maps in the same way we will handle search queries on Google Search under our 18 month logs anonymization policy.

c. *Search queries on Google news;*

In addition to the actual query, we collect standard log information in Google News as that described above when a user enters a query on Google Search. We will handle search queries on Google News in the same way we will handle search queries on Google Search under our 18 month logs anonymization policy.

d. *Search queries on Google images;*

In addition to the actual query, we collect standard log information in Google Images as that

described above when a user enters a query on Google Search. We will handle search queries on Google Images in the same way we will handle search queries on Google Search under our 18 month logs anonymization policy.

e. Email sent, received, or drafted on Gmail;

Gmail is a registration-based service. We ask users for very limited data that we use to protect the security of their accounts. To sign up for a Gmail account, users need only provide a user name (which does not have to be their given name), an alternate email address and the user's country (which we do not verify). To put this into context, registrants for the Yahoo! email service are asked to provide their full name, gender, birthday, existing email address, and zip code. Similarly, Microsoft's Hotmail email service requests a user's full name, gender, year of birth, existing email address, and zip code.

Once a user is authenticated (logged in) and begins to use the service, the user can draft, send, receive and save their emails. When a user deletes an email from Gmail, the message immediately disappears from the user's account view. Because our infrastructure is designed to protect against inadvertent deletions and system failures, residual copies of deleted messages and accounts may take up to 60 days to be deleted from our active servers and may remain in our offline backup systems.

To further empower our users, we designed an "off the record" feature in Gmail's chat service (called Google Talk). While users can save instant messages with their emails, they also have the choice to go "off the record" at any time, in which case the chat messages are never stored on our servers or in either party's archives.

Similarly, we designed portability into Gmail. Unlike most other web mail services, which do not allow users to easily transfer their emails to a different service, Gmail was launched with the ability to export emails and contacts to other email providers. We believe that this openness and transparency is the right thing for our users and consistent with fair information principles. Moreover, this portability feature – which allows our users to easily switch to a competitive service – requires that we continue to offer a superior product and privacy protections that our users value.

The Gmail Privacy Policy is found at gmail.google.com/mail/help/privacy.html.

f. Information or data collected or retained through a website's use of Google Analytics;

Unlike the other products reviewed here, Google Analytics is not a consumer-facing product. Rather, Google Analytics is a service that enables web site owners to improve their marketing campaigns and web pages based on precise and actionable information. Google Analytics itself does not collect or use personally identifiable information, although it is possible for the web site owner to do so. Instead, Google Analytics has only anonymous usage data that is used for statistical reporting back to its web site customers. Moreover, Google Analytics works with first-party cookies for each web site, so that individual web users are not tracked across sites.

g. Information or data collected or retained from an individual's use of Google Desktop Search, including the Google Desktop Search feature, Search Across Computers;

Google Desktop is a downloadable client application that allows a user to search his or her

computer (including documents, music files, and photos) as easily as searching the web with Google Search.

The current version of Google Desktop is enhanced with security and privacy features that guard against phishing, malware and spyware by warning users when they are about to visit a site that might be engaged in stealing personal information or installing spyware on the user's computer. Google Desktop's Lock Search feature enables users to protect themselves by temporarily preventing anyone from doing a Desktop search on the computer. Users can further protect their data by setting their preferences so that the software does not search specific files or folders.

The Google Desktop application only searches on the local computer where the user has stored data; no data is stored on Google's servers unless the user explicitly uploads data files to Google (as described in the Search Across Computers feature below). Users may, however, use Google Desktop to search the web, in which case the searches are stored with a user's Web History (also described below) but can be deleted by the user.

The latest version of Google Desktop provides a Search Across Computers feature, which allows users to search for specified files on their home computer when they are at work, for example. Users must register and be authenticated to use the Search Across Computers feature and must affirmatively elect (opt-in) to use this feature. Files designated by a user who opts-in are stored on Google's servers. If a user deletes a file from a computer using the Search Across Computers feature, that file is deleted from Google's servers within 10 days. Likewise, if a user disables Search Across Computers, the cached versions of the files from the user's computers are deleted from Google's servers within 10 days.

The Google Desktop Privacy Policy is found at desktop.google.com/privacypolicy.html.

h. Google Maps for Mobile;

Google Maps for Mobile (GMM) is a downloadable client application that allows a user to access Google Maps on a mobile device. The current version of GMM does not require user authentication, and we do not collect name, email address, phone number, Google Account information, or other PII when users use GMM.

GMM collects much of the same non-PII as the Google Maps service, though certain information may differ slightly, because the user accesses the service from a mobile device (thus, for example, a query to GMM may include the device type or carrier information). Each download of GMM comes with a unique client ID. The client ID is used to distinguish requests between various downloads of GMM, but does not identify the user. Because GMM is a mapping application, and can be used on a phone with GPS enabled by the user, location information may be sent to us. We do not associate this location information with any PII. The most current version of GMM has a beta feature called My Location. This feature determines the approximate location of the user's mobile device using aggregated and anonymous location information. Users have the option of turning off My Location if they wish.

The Mobile Privacy Policy, governing GMM and other Google mobile products, is found at www.google.com/mobile/privacy.html.

i. Google Web History Program for registered Google users/Google users with sign-in accounts;

Google Web History is a customized service for registered users. When a user signs up for a Google Account, the registration page includes a notice that Web History will be enabled with the account, a link to more information about how Web history works and the simple ability to opt-out of this feature. The Web History feature is fully transparent and allows a user who has signed into his or her account to view and search across the user's history of Google searches, web pages, images, videos and news stories. Users can turn Web History on or off, pause the Web History when they want to, and remove any items from their web history at any time. In short, users have meaningful and granular choices regarding the retention of data associated with their account.

When a user pauses Web History, searches conducted by that user are not stored in association with the user's account. When a user deletes individual searches from Web History, those searches are disassociated from the user's account. When a user disables or signs out of his or her account, searches conducted by that user will not be associated with the user's account as long as the feature continues to be disabled. In each of these cases, the only data retained is the same general non-PII that is logged when an unauthenticated user conducts a Google search. This data will be anonymized in accordance with our recently announced 18-month anonymization policy.

The Web History Privacy Policy is found at www.google.com/history/whprivacy.html.

j. Information or data collected or retained from an individual's use of Picasa;

Picasa is a photo application acquired by Google in 2004, which is available as a downloadable client application for organizing photos on a user's computer (Picasa Software) or, as introduced in 2006, as a Web application for hosting and sharing photos with others (Picasa Web Albums).

A Picasa Software user never has to send or share any personal information with Google; all of their photos can remain solely on their computer. If a user signs up for the Picasa Web Album service, we ask for limited information to create a Google Account (user name, alternate email address and country) and this authentication information is used to secure the account. Authenticated users can upload photos to the service and designate them as either public, public and searchable (photos are searchable on Picasa Web Albums, Google, and other services), or unlisted (photos only viewable to people who have the album URL, which includes an authentication key). When a user deletes photos from the user's account, they become inaccessible to the user and any other viewer.

The Picasa Web Albums Privacy Policy is found at picasa.google.com/intl/en_us/web/privacy.html.

k. Information or data collected or retained from an individual's use of Calendar;

Google Calendar is a registration-based service, and as such we treat the data provided by users – in this case, scheduling and appointment information – in a way similar to how we treat Gmail data and the data of other registration-based services.

When a user signs up for Google Calendar, we ask for the user's time zone in addition to the

limited information (user name, alternate email, and country) requested to create a Google Account. From that point forward, users can add, modify and delete events and comments on their calendars. Users control the privacy settings of these calendars, i.e., they can determine whether it's entirely private (only they can view the events), whether specific individuals can access the event information (or just the free/busy information), and whether the public can view the event information (or just the free/busy information). Events that a user has been invited to by another user may continue to exist in the second user's account even after the first user has deleted the event. Because of the way that we maintain this service, the deletion may not be immediate, and residual copies of your calendar information may remain in our offline backup systems.

We may also record non-PII in order to improve the Calendar service such as the number of events and calendars that a user creates. Every ninety days, if not more frequently, we permanently delete such non-PII usage statistics associated with an individual Google Calendar user. We retain this non-PII beyond 90 days in aggregate form only.

The Calendar Privacy Policy is found at www.google.com/googlecalendar/privacy_policy.html.

1. Cookies.

A "cookie" is a small file containing a string of characters that is sent to a user's browser when the user visits a website. Cookies may store user preferences and other information. When the website is visited again from the browser again, the cookie allows that site to recognize that browser. The user can reset the browser to refuse all cookies, indicate when a cookie is being sent, and delete cookies. However, some website features or services may not function properly without cookies.

For example, Google uses what we call a "PREF cookie" to remember our users' basic preferences in Google Search, such as the fact that a user wants search results in English, no more than 10 results on a given page, or a SafeSearch setting to filter out explicit sexual content. When we originally designed the PREF cookie, we set the expiration far into the future — in 2038, which is the recognized end date for the vast majority of computers operating in Unix time — because the primary purpose of the cookie was to preserve preferences, not to let them be forgotten. We were mindful of the fact that users can always go to their browsers to change their cookie management settings (*e.g.*, to delete all cookies, delete specific cookies, or accept certain types of cookies like first-party cookies but reject others like third-party cookies). After listening to feedback from our users and from privacy advocates, we concluded that it would be a good thing for privacy to significantly shorten the lifetime of our cookies, as long as we could find a way to do so without artificially forcing users to re-enter their basic preferences at arbitrary points in time.

In the coming months, Google will start issuing our users cookies that will be set to auto-expire after two years, while auto-renewing the cookies of active users during this time period. In other words, users who do not return to Google will have their cookies auto-expire after 2 years. Regular Google users will have their cookies auto-renew, so that their preferences are not lost. And, as always, all users will still be able to control their cookies at any time via their browsers.

In addition, we currently plan to begin anonymizing PREF cookies after 18 months beginning in January 2008. We will do this by deleting each PREF cookie's unique ID number.

In connection with our authenticated services, such as Gmail, Google uses a cookie that contains a user's authentication information. This is what allows the user to access the service. These cookies are cleared either when the user logs out, or at the end of the session, or after two weeks if the user chooses to be remembered by clicking "remember me" on the login page.

In our business of contextual advertising, which we describe below in detail, we use cookies for very limited purposes for AdWords and AdSense. For example, we serve a conversion measurement cookie on a per advertiser basis for purposes of measuring conversion. That is, when a user clicks on an ad provided by Google and the user is taken to the advertiser's website, we may serve a cookie to measure whether the user completes a purchase. The conversion measurement cookie is set only for AdWords advertisers that want to engage in conversion measurement; if our advertisers don't want this service, we don't serve the cookie. The cookie is only used for conversion tracking, and on the page where conversion occurs, we provide transparency to users by providing a link to information about the cookie. The conversion measurement cookie expires 30 days from when it is set.

As part of our ongoing effort to better explain to our users in simple, plain language the information we collect and how we use it, we recently launched the Google Privacy Channel on YouTube. One of the videos that we produced (found at www.youtube.com/watch?v=EfqFJb8qkk4) explains cookies to our users. We plan to continue to inform and educate our users about cookies and other components of our service that involve information collection relating to our users' use of our products and services.

2. Please explain how Google uses the information or data described in Question 1(a) – (1), including, but not limited to, the following uses: perfecting Google's search algorithm; operating Google's advertising programs such as AdWords and AdSense; and research or analysis of user activity on www.google.com.

In the context of our search server logs, we retain this data for several reasons.

First, we use this data to improve our search algorithms for the benefit of our users. For example, we receive real-time feedback on the quality of our search results when users click on results. If they click on the first result then we know that we have likely provided them with what they are looking for. If, however, they click far down in the results then our search rankings could be improved.

Second, we use this data to continually improve our services. For example, our spellchecking feature in Web Search is based on an analysis of our search query logs to identify patterns of typos and corrections. By using the logs data, we are able to create extremely accurate spellchecking for a multitude of languages.

Third, we retain this data to defend our systems from malicious access and exploitation attempts, as well as click fraud and web spam. For example, with historical analysis we can identify and protect against patterns of malicious behavior that are hard to identify in real-time. Our retention policies also protect our users from threats like spam and phishing.

Fourth, the server log information is the record of our ad serving and click activity. As such, it is the foundation for our financial reporting and auditing requirements.

Finally, keeping search log data for a reasonable period of time helps us respond to valid legal orders from law enforcement as they investigate and prosecute serious crimes like child exploitation.

3. Please explain the need to retain collected information for the length of time described in your response to Question 1.

In general, we retain collected information relating to authenticated users for as long as the data is useful to the users. For example, we retain emails in a Gmail account for as long as the Gmail account holder wishes to store the emails.

Many parties have asked us why we decided on an 18 month anonymization policy for our search logs. In response to this question, we have described several of the reasons why we retain in particular our search server logs. Security is one of the important factors that went into that decision. In fact, as noted above, we use logs to help defend our systems from search spam, click fraud, and other attempts to compromise or exploit our services.

One of the reasons we need to retain search logs for 18 months is because of cyclical patterns. Some patterns operate on hourly cycles. Some are daily. Others are annual. In order to detect a pattern, we need more data than the length of the pattern. In addition, it is difficult to detect illicit behavior because bad actors go to great lengths to avoid detection. One method of detecting new illicit behaviors is to compare old data with new data. It is generally the case that the older the data the better it is to contrast old patterns with new patterns that may include new and sophisticated illicit behavior.

Even though older data is useful to us, we nevertheless made the decision to retain search logs only for 18 months in the interests of balancing our need to protect our systems' integrity and security – upon which our users rely – with our users' privacy interests. We believe that this is the right balance for our business needs and our users' interests. Although we were the first major search engine to introduce finite retention policies, other companies have followed our lead. Microsoft has since introduced an 18 month retention period for logs and Yahoo! has introduced a 13 month retention period.

4. Please explain how Google uses the information or data described in Question 1(a) – (1), or any additional data, to drive or target advertisements to individual users' computers.

We derive most of our revenues from fees we receive from our advertisers through our AdWords and AdSense programs.

Google AdWords is our automated online program that enables advertisers to place targeted text-based and display ads on our web sites and the web sites of our Google Network members – companies that have web sites on which Google ads appear. Most of our AdWords customers pay us on a cost-per-click basis, which means that an advertiser pays us only when a user clicks on one of its ads.

Google AdSense is the program through which we distribute our advertisers' AdWords ads for display on the web sites of our Google Network members. Our AdSense program includes AdSense for search and AdSense for content. AdSense for search is our service for distributing

relevant ads from our advertisers for display with search results on our Google Network members' sites. Examples of Google Network members that distribute ads from our advertisers with search results include AOL and Ask.com. To use AdSense for search, most of our AdSense for search partners add Google search functionality to their web pages in the form of customizable Google search boxes. When visitors of these web sites search either the web site or the Internet using these customizable search boxes, we display relevant ads on the search results pages, targeted to match user search queries. Ads shown through AdSense for search are generally text ads.

AdSense for content is our service for distributing ads from our advertisers that are relevant to content on our Google Network members' sites. Under this program, we use automated technology to analyze the meaning of the content on the web site and serve relevant ads based on the meaning of such content. For example, a web page on an automotive blog that contains an entry about vintage cars might display ads for vintage car parts or vintage car shows. These ads are displayed in spaces that our AdSense for content partners have set aside on their web sites for our AdWords content. AdSense partners include publishers like *U.S. News and World Report* and the *New York Times*. For our AdSense program, our advertisers pay us a fee each time a user clicks on one of our advertisers' ads displayed on Google Network members' web sites or, for those advertisers who choose our cost-per-impression pricing, as their ads are displayed.

The information that we use to serve ads to individual computers depends on whether the user is searching through Google.com or another search engine or whether the user is viewing content on a Google Network member's web site.

If a user is searching through Google, for example, we provide an AdWords ad based on the following data relating to the user: the current and previous search query entered by the user, the language we believe the user performing the search prefers (based on the Google domain used, user settings, and/or the language of the search query entered by the user), and the IP address of the computer used by the user for an approximate geographic location as assigned by the user's Internet Service Provider or ISP.

If a user is viewing content on a Google Network member's web site, we typically provide an AdSense ad based on the following data relating to the user: the content of the page (*e.g.*, an article about golf), the language of the page's content, and the IP address of the computer used by the user for an approximate geographic location as assigned by the user's ISP.

In either case, both products are contextually targeted, which means that the ads are responsive to what a user types into a search box or the content that the user is viewing.

Our AdWords and AdSense products use limited types of data to serve relevant ads to Internet users. By contrast, other companies' advertising products depend on broader ranges of data. For example, some of our competitors serve ads based on user profiles generated from a combination of search queries, web pages viewed, demographic data provided by the targeted user or by a third party, and other data.

5. In particular, please explain whether Google Maps directs advertisements to IP addresses based on that user's Google Maps search query history.

AdWords ads that appear alongside locations on Google Maps are provided based on the map

location being viewed by the user. These ads do not take into account the search history of an individual user.

6. Please explain how and why information is combined or shared across platforms when consumers opt-in for personalized services and whether Google first requires consent prior to such information-sharing. (For instance, whether search query data is shared with or linked to a user's Gmail account.)

We do combine some data between Google services to improve our users' experience. For example, Google users may use the same Google.com cookie to sign into Gmail, Google Groups, and to save their search preferences on Google.com. This is common practice for any online service that offers a universal sign-in to its users. As noted above, these cookies are cleared either when the user logs out, or at the end of the session, or after two weeks if the user chooses to be remembered by clicking "remember me" on the login page.

However, we do not share search query data with or link such data to a user's Gmail account unless the user has requested that we do so by signing up for the Web History service.

7. Please identify the sections of Google's privacy policy that address the retention and use of the data described in Question 1(a) – (l).

We believe that we provide a very accessible privacy policy that is written in a clear, easy-to-read format, and still provides a substantial amount of detail. This format – known as a "layered notice" format – is embraced by the European Union and used by many Internet companies. It consists of a top-level "highlight" summary of the privacy policy, which then links to a full and detailed privacy policy, policies that are specific to our array of products and FAQs that describe in lay terms things like "what is a cookie?" or "what is a server log?"

Indeed, we provide what is recognized as one of the best descriptions of a server log in our privacy FAQs, found at www.google.com/intl/en/privacy_faqs.html. It actually shows what a log line looks like and breaks down the component parts. We believe it is important for users to understand the data that we collect, and that showing data such as a log line helps achieve this goal.

Descriptions of our use of the data described in Questions 1(a)-(l) are located on the following web pages:

- a. Search queries on Google Search. See www.google.com/privacy.html. It is important to note that our 18 month logs retention policy is not yet reflected in our privacy policy because we are in the process of implementing logs anonymization with the goal of completing search log anonymization by the end of January 2008.
- b. Search queries on Google Maps. See www.google.com/privacy.html and maps.google.com/help/privacy_maps.html.
- c. Search queries on Google News. See www.google.com/privacy.html.
- d. Search queries on Google Images. See www.google.com/privacy.html.

- e. Email sent, received, or drafted on Gmail. See www.google.com/privacy.html and gmail.google.com/mail/help/privacy.html.
- f. Information or data collected or retained through a website's use of Google Analytics. See www.google.com/intl/en_ALL/privacy.html. It is important to note that Google Analytics is a service provided to third parties. As part of our Google Analytics User Agreement, we contractually bind such third parties to (1) not use the service to track or collect PII of Internet users; (2) not allow any third parties to use the service to track or collect PII of Internet users; (3) abide by an appropriate privacy policy and comply with all applicable laws relating to the collection of information from visitors to their web sites; and (4) post a privacy policy that provides notice of its use of a cookie that collects anonymous traffic data.
- g. Information or data collected or retained from an individual's use of Google Desktop Search, including the Google Desktop Search feature, Search Across Computers. See www.google.com/privacy.html and desktop.google.com/privacypolicy.html.
- h. Google Maps for Mobile. See www.google.com/privacy.html and www.google.com/mobile/privacy.html.
- i. Google Web History Program for registered Google users/Google users with sign-in accounts. See www.google.com/privacy.html and www.google.com/searchhistory/privacy.html.
- j. Information or data collected or retained from an individual's use of Picasa. See www.google.com/privacy.html and http://picasa.google.com/intl/en_us/web/privacy.html.
- k. Information or data collected or retained from an individual's use of Calendar. See www.google.com/privacy.html and http://www.google.com/googlecalendar/privacy_policy.html.
- l. Cookies. Because cookies are not products, we do not have a separate privacy policy relating specifically to each of the types of cookies that Google uses to provide services to users. We do explain cookies in our Privacy FAQs (www.google.com/privacy_faq.html), disclose our use of cookies in our privacy policy (www.google.com/privacy.html), and we provide our own and user-generated content on the Google Privacy Channel on YouTube (www.youtube.com/googleprivacy) that explains cookies to users. We also explain cookies that we serve in connection with our test ad server at www.google.com/ads/gcc_privacy.html.

We continue to innovate to provide better information to our users about privacy. For example, we recently created the Google Privacy Channel, we are using the Google Blog to communicate with our users and the privacy community about privacy issues, and we continue to produce Google privacy videos that explain our privacy policies in simple, plain English. The Google Privacy Channel is found at www.youtube.com/googleprivacy.

These steps are all part of our ongoing effort to reach our users in meaningful ways about the privacy decisions they make.

8. Please explain the technology called “rich media” or “interactive multimedia,” how this technology works, and what information may be collected by its use.

“Rich media” are media that have been enhanced with animation or video. The term is particularly relevant in the context of online advertising. Rich media ads are animated, and often streamed, so that they appear more like television commercials, as opposed to ads containing static images and text. Because we serve a very limited number of rich media ads, this is not an area where we have much experience. Other companies have longer track records of and a sharper focus on offering these ads.

Though we provide a very limited number of rich media ads, in September, we announced the introduction of Google Gadget Ads, a new interactive ad format that is currently in an expanded beta test with a segment of AdWords advertisers. Gadget Ads – which have rich media capabilities – enable advertisers to target audiences in a flexible and timely manner via regular updates within the ad unit, and also allow users to engage with ad content in a way that static ads have not facilitated in the past. Gadget Ads can incorporate images, video, and other features in a single creative unit and can be developed using Flash, HTML, or a combination of both.

The information we collect when we serve a rich-media ad to an AdSense publisher site is similar to the information that we collect when we serve text or static ads. Indeed, we specifically prohibit advertisers from directly capturing personally identifying information, such as email addresses, telephone numbers or credit card numbers. We also prohibit the use of gadget ads to create or read any cookies on ad impressions or interactions or for web beacons, pixel tags or other similar tracking mechanisms.

9. Please explain whether Google utilizes such technology.

As noted above, though we do serve rich media ads, this is a very limited part of our advertising business, which consists primarily of offering text ads.

10. Please explain whether Google posts a link to its privacy policy on the home page or search results page of www.google.com and, if not, explain why not.

When a registered user accesses his or her customized iGoogle page, a link to Google’s privacy policy appears at the bottom of the home page. Unregistered users of google.com, users accessing google.com through the Classic Home page and/or users who have not logged in can access Google’s privacy policy by clicking on “About Google.”

11. In Google’s privacy policy, “personal information” is defined as “information that you provide to us which personally identifies you, such as your name, email address, or billing information, or other data which can be reasonably linked to such information by Google.”

a. Please describe how Google interprets “reasonably linked.”

Personal information, or personally identifying information, has been defined in a variety of ways. Information that specifically and directly refers to someone (*e.g.*, their name, email address, and billing information) is personal information. In addition, information that can be combined

with readily available information to identify a specific individual is also generally considered personal information. We use the phrase “reasonably linked” to describe this second category of personal information. Whether something can be “reasonably linked” to an individual depends on the circumstances (what the data is and what other data the viewer of that data has), and is likely to change as technology evolves. When an individual is not authenticated, we do not consider an IP address to be personally identifiable because we would need to get specific data from an ISP about which of its customers was using a particular IP address at a particular time on a particular day in order to link it to an individual. Even then, you could not say which member of a household was online at a particular time.

In sum, whether information can be “reasonably linked” to an identifiable individual turns on (i) what the data itself is – and in particular how frequently it accurately and reliably describes an individual; (ii) what kind of additional information is needed to identify the specific person to whom that data relates; (iii) who has access to the additional data needed; and (iv) the circumstances under which the additional data will be made available to others.

b. Please explain in what circumstances Google links information such that an individual can be identified.

Google does not actively try to cross-correlate information in order to try to specifically and directly identify an individual. Rather, the amount of identification a user has while using Google products and/or services is in the sole discretion of the user. A user may register for Google products and services using his or her actual name or by using an anonymous name. Moreover, a user can use Google.com as an anonymous user or the same user can register and use Google products and services as an authenticated user. The “reasonably linked” language is more protective of users and designed to hold Google to a higher standard *if* we find ourselves in a situation where non-PII becomes PII.

c. Please explain whether Google considers an IP address to be “personal information.”

There is an important distinction between personally identifiable and non-personally identifiable information. This makes sense because the level of sensitivity of information that would identify an individual, such as the person’s name and social security number, is very different from the sensitivity of a zip code without any additional information that ties the zip code to a person. An IP address cannot necessarily be tied to any individual user or even to an individual machine – multiple unrelated users can easily show the same IP address in their web requests.

d. Please explain whether technology exists to personally identify or determine the personal characteristics, including, but not limited to, name, email address, physical address or location, age, gender, or ethnicity of an Internet user based on that user’s IP address.

To our knowledge, no technology exists today that would allow any party to identify with certainty any individual’s name, physical address or location, age, gender, or ethnicity through an IP address. What an IP address tells us is the general physical location of a computer that is being used to access our services. Sometimes IP addresses do not even do that, and ultimately how much we know about the location of a computer associated with an IP address depends on how an ISP through which the computer accessed the Internet has assigned IP addresses to its customers.

Moreover, given increasing mobility and the prevalence of easy to use portable devices, the connection between where a computer is and who is using that computer becomes increasingly unreliable.

e. Please explain whether Google is capable of identifying or determining personal characteristics, including, but not limited to, name, email address, physical address or location, age, gender, or ethnicity of an Internet user based on that user's IP address.

As noted above, Google does not have the capacity to identify personal characteristics such as name, physical address or location, age, gender, or ethnicity based solely on an IP address.

12. Please define the term "anonymization" as related to the data collected as described in, but not limited to, Question 1(a) - (l).

To us, anonymization means that we have reasonably separated a data element from the specific machine or host in a network that was connected to such data element and thus eliminating any possibility of attaching an IP address to an individual computer or host network.

For example, as noted above, we plan to anonymize our search logs by January 2008. What this means is that we will delete the last octet, typically one to three digits of the IP address contained in the log that identifies a specific machine or host network and fully erase the unique ID number of the cookie associated with the log. Some have pointed out that the deletion of the last octet of an IP address ought to be characterized as pseudonymization rather than as anonymization because we do not plan to delete the full IP address. However, as discussed above, it is difficult today to connect an IP address in our servers to an individual person, and the deletion of the last octet of the IP address significantly reduces the possibility of making such a connection by increasing significantly the number of computers that could be associated with an IP address.

We have chosen to not delete the whole IP address after 18 months because our analysis of large amounts of aggregated data is very useful for improving the security and quality of our services.

13. Are Google's practices described in response to Question 12 consistent with industry-wide practices? If not, please describe any variance.

Google is an industry leader in the effort to protect user privacy by anonymizing search logs, and we were the first leading search company to announce publicly the anonymization of such logs after 18 months. Prior to this year, search companies did not disclose publicly their search log retention policy. As a result of our decision, other search companies have moved to establish and make public their own search log anonymization policies. The Center for Democracy and Technology recently released a survey of these practices, and characterized them as "great news for users." (See www.cdt.org/privacy/20070808searchprivacy.pdf.) Though some companies may retain search logs for shorter periods of time, we believe that our anonymization policy accomplishes the goals of improving our services, protecting the integrity and security of our systems, and protecting the privacy of our users.

14. Please describe how Google anonymizes IP addresses.

We plan to anonymize IP addresses that form part of our search logs by deleting the last octet –

the last one to three digits that typically identifies a specific computer or host network – of each address. For example, if the IP address of a computer is 66.249.72.110 at the time that a user searches with Google Search from that computer, then 18 months after the search query is entered we plan to delete “110” from the IP address. Though we have not yet anonymized IP addresses in our server logs, we plan to do so by January 2008 and we plan to make this change retroactive.

15. *Please describe how Google anonymizes cookie data.*

We plan to anonymize cookies that form part of our server search logs by deleting the ID number of each such cookie. For example, if a cookie that we serve to a computer at the time that a user searches with Google Search from that computer is assigned the number 740674ce2123e969, then 18 months after the search query is entered we plan to delete that unique cookie ID number in its entirety. Though we have not yet anonymized these cookies, we plan to do so by January 2008 and we plan to make this change retroactive.

16. *Please explain whether Google has the capability or has attempted or plans to attempt to combine or merge the data described in Question 1(a) – (l).*

The optional Web History feature described above saves and combines information from several of the listed services. Specifically, a user’s searches and activity on Web Search, Images, and News all become part of the user’s online Web History if the user chooses. This personal search history is available for the user to review and control, including by deleting specific searches or pausing the Web History feature for a period of time.

17. *Please define tracking cookies, which may track users across multiple websites, and how they function.*

Online ad-serving technology can be used by advertisers to serve and manage ads across the web. In order to provide such service, the ad server sets a cookie on the user’s computer browser when the user views an ad served through the ad server. That cookie may be read in the future when the ad server serves other ads to the same browser. DoubleClick, which is an ad serving company and a founding member of the Network Advertising Initiative (NAI), allows users to opt out of the ad-serving cookie by visiting the NAI’s website. Google is currently applying to become a member of NAI.

18. *Please explain whether Google uses the tracking cookies described in response to Question 17. If the answer is no, please describe how Google’s cookies are distinct from those described in Question 17.*

Google is testing a new ad serving technology, and the privacy policy describing the cookies set in connection with that technology, their use and how users can opt out of the cookie is found at www.google.com/ads/gcc_privacy.html.

19. *Please explain whether Google’s cookies reset and, if so, how and when the cookies reset.*

As noted above, Google uses our so-called “PREF cookie” to remember our users’ basic preferences, such as the fact that a user wants search results in English, no more than 10 results on a

given page, or a SafeSearch setting to filter out explicit sexual content. When we originally designed the PREF cookie, we set the expiration far into the future — in 2038, to be exact — because the primary purpose of the cookie was to preserve preferences, not to let them be forgotten. We were mindful of the fact that users can always go to their browsers to change their cookie management settings to, for example, delete all cookies, delete specific cookies, or accept certain types of cookies (like first-party cookies) but reject others (like third-party cookies).

After listening to feedback from our users and from privacy advocates, we've concluded that it would be a good thing for privacy to significantly shorten the lifetime of our cookies — as long as we could find a way to do so without artificially forcing users to re-enter their basic preferences at arbitrary points in time. And this is why we're announcing a new cookie policy.

In the coming months, Google will start issuing our users cookies that will be set to auto-expire after 2 years, while auto-renewing the cookies of active users during this time period. In other words, users who do not return to Google will have their cookies auto-expire after 2 years. Regular Google users will have their cookies auto-renew, so that their preferences are not lost. As always, all users will still be able to control their cookies at any time via their browsers.

20. If the merger of Google and DoubleClick is approved, please describe what use Google plans to make of the data retained and collected by DoubleClick (for example, data from DoubleClick's tracking cookies or DoubleClick click-stream data), and whether Google plans to combine or merge DoubleClick's data with data Google retains from individual search queries and other user activity on www.google.com.

We have not completed the acquisition, and we are new to the third-party display ad serving business, so we have not yet decided whether or how we would merge DoubleClick and Google data. We do know that combining Google and DoubleClick data would involve certain technical and legal issues. For example, we understand that we would need DoubleClick's advertising customers' consent to use their data in such a fashion before taking any action. We also know that consumers, publishers and advertisers could benefit from merging some portions of the data in the future. These benefits include more relevant and tailored ads for users, and better reporting on ad effectiveness to advertisers and publishers. Finally, we know that any merging of data would have to be done in a way that protects the privacy and security of our users, an endeavor to which we are deeply committed.

a. If Google does not intend to merge or combine the data Google retains with the information or data retained or collected by DoubleClick, please describe the efficiencies of the Google-DoubleClick merger.

As noted above, we have not completed the acquisition, and we are new to the third-party display ad serving business, so we have not yet decided whether or how we would merge DoubleClick and Google data. However, the Google-DoubleClick merger presents numerous efficiencies unrelated to any data that DoubleClick collects. In fact, the data that DoubleClick collects via its cookies was not a factor in our decision to pursue the merger.

For instance, acquiring DoubleClick's expertise in display ad serving will assist Google in its efforts to design an integrated interface for advertisers to manage their text and display advertising campaigns. In addition, the acquisition will allow Google to provide advertisers with better metrics

for the display ads they place in our advertising network. DoubleClick's display ad serving business will also help Google provide publishers with improved choices for monetizing their inventory, as our AdSense partners will become able to better serve and monitor the effectiveness of display advertising on their properties. Most importantly, we believe that the combination of DoubleClick's ad serving technology with Google's expertise in contextual targeting will lead to consumers receiving more relevant online advertisements.

b. If Google does not intend to merge or combine the data Google retains with the information or data retained or collected by DoubleClick, please explain how the information will be segregated.

As noted above, we have not completed the acquisition, and we are new to the third-party display ad serving business, so we have not yet decided whether or how we would merge DoubleClick and Google data.

21. Please describe how Google defines "behavioral targeting."

Despite much discussion across the industry, we are not aware of any strict definition of behavioral targeting. This may be in part because of the broad range of practices in online advertising that span from the use of many types and significant quantities of behavioral and demographic data as signals for serving advertising to very limited information used to target advertising. Some companies use demographic data ranging from age, gender and household income to psychographic data such as attitudes and beliefs of consumers to target advertising. Others are using search queries, demographic data and other historical behavioral data such as emails and web surfing habits to target ads to users. As was described above, Google comparatively uses very limited types of data.

22. Please describe your understanding of the broader industry's definition of "behavioral targeting."

We do not believe that there is a broad industry definition of behavioral targeting or behavioral advertising. However, on December 20, the FTC issued a set of proposed principles entitled "Online Behavioral Advertising Moving the Discussion Forward to Possible Self-Regulatory Principles." In the proposal, the FTC defined "behavioral advertising" as the tracking of a consumer's activities online "including the searches the consumer has conducted, the web pages visited, and the content viewed – in order to deliver advertising targeted to the individual consumer's interests."

23. Please describe Google's understanding of the Asia-Pacific Economic Cooperation (APEC) guidelines and how the guidelines would apply to Google's practices, including, but not limited to, those functions described in Question 1(a) - (l).

The APEC Privacy Framework was inspired by the OECD Guidelines on the Protection of Privacy and is concerned with ensuring consistent and practical privacy protection across a wide range of economic and political perspectives.

While Google sees the potential for the APEC Privacy Guidelines to serve as the framework for a global privacy framework, in Google's current business practices, Google complies with the law of

the jurisdiction in which it is conducting business. For example, in the U.S., Google complies with U.S. privacy laws and the obligations placed on it by its Safe Harbor Certification and in the EU, Google complies with the EU Data Protection Directive of 1995.

Google's support for the APEC privacy principles has been to help raise privacy protections in the many countries around the world where there are no current privacy protections.

24. The House passed the Securely Protect Yourself Against Cyber Trespass (SPY ACT) in the current and prior two Congresses. The SPY ACT, H.R. 964, sponsored by Representatives Mary Bono and Adolphus Towns, mandates an opt-in privacy regime by prohibiting the collection of personal information from a computer without a user's notice and consent prior to the execution of any information collection program. H.R. 964 also demands that a user be able to easily remove or disable the information collection program. Please explain whether Google's applications are subject to H.R. 964's consent requirements. If the answer is no, please explain why these programs, which collect personal information, are not subject to the consent regime established by H.R. 964.

We very strongly support the SPY ACT's goal of eliminating spyware, malware, deceptive adware, and other malicious software that is inadvertently downloaded onto a consumer's computer. In fact, there is significant alignment between the act's goals and the way that Google designs and distributes its software applications.

In 2004, we first outlined a set of software principles that we believe our industry should adopt, and we've shared them publicly to help foster discussion and help address the harm caused by spyware and other malicious software. We follow these guidelines ourselves with the applications we distribute to our software. For example, our principles state that software should not trick a consumer into installing it. We also believe that, when an application is installed or enabled, it should inform users of its principal and significant functions. It should also be easy for a consumer to figure out how to disable or delete an application, and, if an application collects or transmit personal information such as an address, the user should know. Finally, we believe that application providers should not allow their products to be bundled with applications that do not meet these guidelines. Google's software principles are available to the public at www.google.com/corporate/software_principles.html.

Because we feel a responsibility to fight spyware, we also sponsor StopBadware.org, a "neighborhood watch" campaign aimed at fighting spyware and other malicious forms of software. In addition, our search results provide users notice when we believe that a website listed in the results provided to a user has been infected with malicious software.

Under section 3 of the SPY ACT, we would be obligated to provide notice before transmitting an "information collection program" (as defined in the act) to a user's computer and prohibited from executing such a program on the computer without consent. We have not determined conclusively whether any of our downloadable client applications would be subject to Section 3, but we certainly believe that downloadable applications ought to provide notice, and that our applications provide disclosure that is consistent with the requirements of section 3 of act. Google Toolbar is an example of our commitment to and leadership in providing our users with transparency and choice. First, Toolbar doesn't download or install without the user's permission or without giving the user information and choices regarding Toolbar. Second, prior to installation of

Toolbar, the user has the option to opt into receiving PageRank information in the user's toolbar. PageRank stores the sites that have been visited by the browser that the Toolbar is enhancing, much in the same way a browser stores a user's web surfing history. The disclosure in the notice is very clearly presented to the user before confirming that choice, with text that states in bold, red, and upper-case letters, "PLEASE READ THIS CAREFULLY. IT'S NOT THE USUAL YADA YADA," in order to underscore the importance of reading the disclosure.

We continue to see too much spyware and other malicious software that, for example, hijacks browsers from the sites that consumers are trying to visit, and we welcome congressional efforts to address this problem legislatively in a way that helps stop the installation of malicious software on consumers' computers while encouraging continued innovation on the Internet.