Comments of Google Inc.

February 18, 2011

Re: Preliminary Staff Report on "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers"

Via electronic filing: https://ftcpublic.commentworks.com/ftc/consumerprivacyreport/

Google appreciates the opportunity to comment on the work the Federal Trade Commission has done and continues to do to advance consumer protection. The Commission has been instrumental in discouraging practices that are harmful or deceptive and undermine user trust. The Commission has also used its position to effectively champion principles for consumer protection and help guide industry toward establishing best practices.

As the Commission examines how best to protect consumers in an era of rapid change with the release of its report this past December, the fast-paced introduction of new Internet products and services continues to drive rapid shifts in consumer expectations and preferences. Google supports the Commission's promotion of a framework to guide the privacy efforts of all commercial entities, coupled with continued consumer education and enforcement against bad practices.

We offer these comments to highlight how the Commission's proposed framework can help strengthen privacy practices and how Google has incorporated the framework principles into our offerings:

- **Embracing privacy as a fundamental product development concept.** Providers should incorporate consumer privacy into product and service development, and promote it within the culture of the business. At Google, privacy is fundamental in the products we build -- including industry-leading encryption, security tools, and user choice mechanisms. Just last week, we launched 2-step verification for consumer Gmail accounts, which offers users who are concerned about hacking or unauthorized use of their account an extra level of protection.

- **Simplifying consumer choice.** Too often, consumers are unaware of choices, or confused by them. Google agrees that simple, clear choice mechanisms are absolutely necessary to empower users with respect to disclosure, transfers, or sensitive uses of personal data. This is the basis of tools like our Ads Preferences Manager and Dashboard, which are featured in our Privacy Center. In fact, we recently launched our open-source Keep My Opt-Outs browser extension, which enables users permanently to opt out of interest-based advertising.

- **Increasing transparency.** Increasing the transparency of data practices, including streamlining privacy notices and providing reasonable access to consumer data, is key to helping users stay informed about sharing data with providers. We recently simplified our written privacy policy using clearer and shorter prose for just this reason; we provide our users with tools like Dashboard to show what information we have about a user, and Ads Preferences Manager to make it clear what information we might use to provide ads.

- **Educating consumers about data practices.** This is an area of clear common ground, on which the Commission and providers can work cooperatively to empower consumers. Google is proud of the educational efforts we have engaged in, including our curriculum developed with iKeepSafe to teach teens to recognize online risks. But much more can be and must be done.

We also offer suggestions in response to some of the Commission's specific requests for comments. We look forward to working with the Commission further on this vital issue.

I. Privacy Framework

The privacy framework set forth in the Commission's preliminary report presents a helpful lens through which those developing products and services may view and analyze their practices, and for consumers and other stakeholders to evaluate how well providers are protecting personal information. Such a framework, developed further via standards and collaborative processes, can provide commercial entities with both guidance and flexibility to implement privacy principles like transparency, choice, and security in a manner that is sensitive to context and responsive to consumers' evolving expectations.

We are gratified to see that Google's approach to privacy in many key respects follows the framework presented in the Commission's report. We discuss the elements of the Commission's framework below and how providers and other stakeholders can embrace these principles in the development of standards and best practices.

A. Embracing privacy as a fundamental product development concept

The Commission's report highlights the idea that companies should incorporate consumer privacy into product and service development, and promote it within the culture of a business. We agree. This principle is fundamental to protecting personal information. Below, we offer our thoughts on how standards and best practices can develop to better match this principle, with examples drawn from Google's practices.

i. Incorporating technological safeguards to protect data

As part of advancing privacy as a product concept, the report recommends that companies incorporate data security features into their practices. Strong security practices are vital for entities that collect or store personal data, and they address an area where consumers often voice their strongest privacy concerns -- fear of harms such as identity theft, viruses, and phishing. Google supports the excellent work the Commission has done applying its current authority in this area, which has given clear guidance to the industry. We also support passage of a national breach disclosure and security standard.

At Google, we find that integrating data security concerns into our offerings is fundamental to protecting consumer data, which in turn is essential to maintaining user trust. To this end, Google is dedicated to keeping user information secure and to working together with a large community of users, developers, and external security experts to make the Internet safer and more secure. Security is also one of Google's five foundational privacy principles.

Our commitment to security is reflected in our products and services. For instance, we built Google Chrome with security in mind from the browser's inception. Chrome's security features include safe browsing (warns users of sites suspected of phishing or containing malware), sandboxing (prevents browser processes from harming or infecting other processes on the computer), and automatic

updates (delivers security upgrades quickly and uniformly). Google is also the only major search provider that enables users to encrypt search queries. Additionally, as the report notes at page 45, Google remains the only major webmail provider to offer session-wide SSL encryption by default, which protects Gmail users worldwide from improper access to or surveillance of their communications. In the past year, Google launched a new system that notifies users about suspicious activities associated with their accounts. Google also built privacy features into the location sharing settings in Chrome and our Android operating system.

We recently released 2-step authentication for consumer Gmail accounts, which allows users who are concerned about the security of their account to use a password plus a unique code generated by a mobile phone to log in. This is an extra step, but it is one that significantly improves the security of a Google Account. Now, if someone steals or guesses a Gmail user's password, the potential hijacker still cannot sign in to the user's account because the hijacker does not have the user's phone. We are already hearing stories from users about how this extra layer of security has protected them from hacking or unauthorized access.

These are just a few of the privacy and security features that Google has designed as part of our products. We feel that each is an important part of helping users protect their privacy and look forward to more innovation in this space.

ii. Promoting consumer privacy through corporate culture and internal safeguards

As consumers become more reliant on services provided by third parties, consumer privacy relies increasingly on those parties' internal practices, process, and controls. At Google, we understand our responsibility to our users and continually strive to improve our privacy process. As Google recently explained, we have begun to implement even stronger privacy controls with a focus on three prongs: (1) people, (2) training, and (3) compliance.

With respect to people, Google appointed a Director of Privacy, Dr. Alma Whitten, across engineering and product management to manage the process of building effective privacy controls into our products and internal processes. In Dr. Whitten's own words, privacy is "something we think about every day across every level of our company. Why? Because privacy is both good for our users and critical for our business."

We have developed a review process where all engineering projects leads are required to submit and maintain a Privacy Design Document detailing how their projects handle user data. These documents are reviewed by cross-functional working groups that can request code reviews and make recommendations to the product teams. Completion of privacy design documents will also be reviewed by managers and an independent internal audit team.

As for training, in addition to providing new employees with training on Google's privacy principles and requiring them to sign Google's Code of Conduct at orientation, we also enhanced our core training for engineers and others to create a greater focus on responsible collection, use, and handling of data. The process also includes training improvements, such as providing a new information security awareness program to our employees, and focusing on how to develop products that respect the Google privacy principles. Each of these highlights the importance of privacy for Google's corporate culture, and ensures that our employees understand that user privacy is a priority.

Because maintaining user trust is one of our priorities, Google continually reassesses our internal procedures to see how we may better serve our users.

iii. Limiting data collection to legitimate business needs and implementing reasonable retention periods

The Commission has also considered the notion that companies should limit data collection to fulfill specific legitimate business needs and has recommended implementing reasonable and appropriate data retention periods. As the Commission explores ways to structure this aspect of the framework, Google notes that we have found that users benefit significantly from a privacy approach that protects users and encourages understanding and control yet preserves the benefit of new and innovative uses of data. Google is pleased to see the Commission endorse the value of data on pages 21 and 33 of its privacy report. We encourage the Commission to build this concept more directly into its final framework.

Creative and even serendipitous re-use of data has enabled enormous advances in online products and services, which in turn have supported societal benefits such as creativity, education, business growth and job creation, and deepened social and political engagement. From Google's experience alone, re-use of existing data has delivered enormous value to Google users and has led to product improvements such as Gmail's priority inbox; automated spell checking of search terms; search auto-complete; spam, fraud, and virus protection tools; and the development of new services such as FluTrends and Translate.

Where users do not or cannot have adequate controls over personal information or lack a direct relationship with the provider, shortened retention periods and other limitations have more obvious application. It is in part for this reason that Google does not transfer personally identifiable information to third parties without a user's consent, and never sells a user's personal information to anyone. This is also the reason why we voluntarily de-identify unauthenticated data, like our search logs, after a period of time. In contrast, where a user has meaningful transparency and control over her information, arbitrary limitations on retention or new uses of data are less necessary.

B. Simplifying consumer choice

Turning to the foundational principle of choice, the Commission's report recommends that companies simplify consumer choice. Google supports this goal as absolutely necessary to empower users with respect to disclosure, transfers, or sensitive uses of data. To this end, Google provides consumers with an array of easy-to-use control and choice options.

i. A new take on "choice"

The report moves away from the binary opt-in/opt-out vocabulary prevalent in privacy discussions and instead focuses on ensuring that options and information are readily available for those wishing to exercise choice. Google welcomes this shift as a more adaptable way of approaching the principle of user control. We believe that providing users with choice is vital, but that opt-in consent is not a panacea to supplant meaningful user choice.

While the metrics of opt-out usage cannot alone determine its usefulness or validity, Google's experiences with our offerings show that the quality and clarity of user controls are key to their utility. Since Google introduced our Ads Preference Manager, we have seen that for every visitor that opts out, seven users view or edit their settings and choose to remain opted in. More than 100,000 Google users visit Dashboard every day, of which over 80 percent are typically new visitors. Approximately four out of five Dashboard users spend significant time on the site and learn about the information they are storing with Google. One in five Dashboard users typically click through at least one of the links, potentially to change the settings in a particular product. These numbers -- in addition to confirming the importance of offering clear controls -- demonstrate to us that users

become more comfortable with data collection and use when they see that it happens on their terms and in full view.

As a key component of choice, Google also offers portability to our users through our Data Liberation Front, which allows our users to "liberate" their data from more than 25 Google products where users create and store personal information if they choose to switch to other providers or cease using one of our many offerings. We believe that for choice to be meaningful, users must have the option to leave a service if they decide a provider is not meeting their needs. Such portability prevents service providers from becoming complacent and incentivizes them to develop better products to preserve and expand their user base.

ii. Industry Do Not Track mechanisms for interest-based advertising

When addressing choice mechanisms, the report singles out online behavioral advertising, also called interest-based advertising ("IBA"), and asks about the utility of a mechanism to help consumers make a consistent, persistent choice to opt out of the use of IBA profiles or tracking. We think it vital for the Commission, industry, and other stakeholders to continue to engage on improving solutions for users in this area, lest bad actors and confusing practices create distrust in advertising-supported services.

Long before the current discussion about "Do Not Track," Google was offering an industry-leading transparency and control tool for its IBA system. The Ads Preferences Manager, available in our privacy center and via icons placed in every ad on the Google ad network, permits users to opt out of Google interest-based ads services altogether. Google implements this opt-out preference by writing the text "OPTOUT" where a unique cookie ID would otherwise be set. This means that Google cannot form a profile for opted-out users or track a specific browser via our ad network. Google's engineers also developed extensions for all major browsers to make our opt-out cookie permanent, even when users clear other cookies from their browser. We have been delighted to see this style of transparency and control catch on in the industry.

In January, Google sought to further encourage consistency and ease of control over IBA by launching the Keep My Opt-Outs Chrome extension, which enables all providers participating in ever-expanding industry self-regulatory programs to make their IBA opt outs *permanent* via a simple, browser-based mechanism. As new opt outs come online, we will automatically update this extension to keep users up to date. In the first few weeks alone, more than 80,000 users have already installed and are using the extension. We even released this tool on an open-source basis so that other developers can examine, assess, enhance, or even extend the code's capabilities. Already, we have seen third parties adapting the code to create additional or alternative tools. Additionally, we are developing versions of Keep My Opt Outs that work on other major browsers.

While there are many options emerging for consumers to set a Do Not Track preference, we applaud the Commission for recognizing that any solution to this issue must recognize that advertising is the primary means of support for free content on the Internet. All stakeholders should agree that Do Not Track can be achieved without large-scale blocking of third-party content, including advertising. Blocking such content would have a significant, unintended economic cost -- particularly borne by small publishers.

Given the implementation questions and complexity of this issue, we recommend that the process would benefit from review in an open standards body to determine the expectations and responsibilities of all stakeholders. In addition, the Commission should actively use its current enforcement authority to pursue deceptive representations to users or harmful practices.

C. Increasing transparency

The report recommends that companies increase the transparency of their data practices. In particular, the Commission focuses on streamlining privacy notices and providing reasonable access to consumer data. This principle is key to helping users understand the data that is kept on their behalf and about them by providers. As we illustrate below, both the notice and access components of transparency for users have been priorities for Google.

i. Improving privacy notices

While recognizing the value of privacy notices as tools for accountability, the report recommends that companies consider presenting clearer, shorter, and more standardized notices to better enable comprehension and comparison of privacy practices. There is a growing recognition that privacy policies used by companies today are often overly legalistic and more must be done to provide users with an understanding of what data a company or website collects or uses.

Google embraces this notion of transparency, and we have recently simplified our written privacy policy with clearer and shorter prose to ease comprehension for consumers. Additionally, we have sought to increase understanding of privacy practices via other formats, including through videos and FAQs, and have organized these tools under a single Privacy Center. We also provide our users with notice directly in-product, like "tool tips" that show the privacy impact of a particular action or other relevant information.

ii. Providing reasonable access to consumer data

The Commission also recommends that companies provide consumers with reasonable access to data they provide or generate. This is an important goal -- users should remain in control of their data to the extent feasible, which requires the ability to access and see what data providers retain. We have taken this goal to heart. Through such tools as Google Dashboard and our Ads Preferences Manager, we provide users with granular access to the data they give us. In fact, we have discovered that good transparency seems to help users become more comfortable with the use of their data. As we discussed above, for every person that opts out of IBA on our Ads Preferences Manager, *seven* view their settings and remain opted in. This suggests that many users find interest-based advertising to be useful, when it is relevant to their interests and they are given tools to better communicate their preferences.

The Commission should consider transparency in another aspect as well -- transparency about how data is disclosed to third parties. Google is the only major online provider to give users (and the public) access to information about Government Requests for data about users and requests for Google to take down or censor content. This is part of our Transparency Report, which also includes links to graphs that provide information about traffic to Google services around the world, giving up-to-the-hour information about how traffic in a given country might be shaped. It is our hope that this data can help facilitate studies about service outages and disruptions, and encourage Internet freedom worldwide.

D. Educating consumers about data practices

The report asks all stakeholders to expand their efforts to educate consumers about data practices. Google agrees with the Commission that education and user awareness are necessary precursors for users to make effective privacy choices. There are more tools and options than ever for users to take control of their personal information, but without understanding and education for users, they won't

be used fully. Moreover, many young people or new online users need simple ways to learn about and understand the implications of, for instance, sharing information on social networking sites.

To this end, Google engages in a variety of educational initiatives to promote transparency and to educate our users about staying safe online. To help increase adoption of our safety tools and educate families about responsible Internet use, we developed a curriculum with iKeepSafe that teaches teens to recognize online risks, investigate and determine the reliability of websites, and avoid scams. We are distributing the curriculum through the Google Teacher Academy. We will continue to work with various stakeholders to think of ways to improve protections for kids and teens online.

As we discussed above, Google's Privacy Center and educational videos inform our users in plain English what data we store and how we use it. Our Family Safety Center also helps families make choices about how their children use our services. Additionally, Google has partnered with the Commission and others (*e.g.*, child safety organizations) to distribute information about navigating the Internet safely. We also use our blogs and outreach efforts to feature postings that direct Google users to Commission initiatives, including the Commission's Admongo and NetCetera initiatives, as well as other resources to help keep Internet users safe and informed.

We would encourage more work in this regard, including cooperative efforts with the Commission and other agencies, industry organizations and consumer groups. This is an area of clear common ground.

II. Suggestions for the Framework

In response to the Commission's request for specific comments on areas for improvement or refinement, we offer the below observations.

A. Scope of the framework

Google appreciates the technology-neutral approach the Commission has taken with its preliminary Report. We urge the Commission to continue promoting a framework that addresses all kinds of data collection and use, whether online or offline, first party or third party, passively collected or actively solicited from consumers.

From a practical perspective, for example, the distinction between online and offline data is increasingly less helpful for companies seeking to organize and analyze their practices. Moreover, platform- or technology-specific regulations can cause bad practices to migrate to unregulated models, defeating the purposes of regulation and disrupting the market. Google therefore favors approaching privacy issues comprehensively rather than distinguishing among business models.

We further urge the Commission to directly include government access to personal data as they consider a framework for consumer privacy. Google supports stronger protections pertaining to government access to user data and communications. Regarding the Electronic Privacy Communications Act ("ECPA") in particular, we have significant constitutional concerns about a law that permits government access to the content of communications with less than a warrant. For this reason, Google is a leading member of and supports the proposals advanced by the Digital Due Process Coalition to update ECPA in a manner that ensures its protections are consistent with privacy expectations and constitutional requirements. The Commission should serve its consumer protection role by actively urging Congress to action on this issue.

B. Considering the identifiability of personal data

The Commission has inquired how the framework should apply to data that can be reasonably linked to specific consumers, computers, or other devices, or that may become linkable in the future. Additionally, the Commission has asked whether there are reliable methods for ascertaining whether a particular dataset is linkable, and whether there are technical means to "anonymize" data. These questions suggest that the Commission is grappling with the notion of what data may be "identifiable" and what data should be covered by the framework.

We agree that the traditional concept of personally-identifiable information -- as a dividing line between protected and unprotected information -- is incomplete. All data derived from individuals, whether personally-identifiable data or not, deserves some manner of protection. Yet the distinction between PII and non-PII still presents an important distinction. Rather than apply identical protections to all categories of data, it is important that any framework proposed by the Commission is properly calibrated to fit different categories of personal data.

Google believes that privacy principles, including standards for choice, may apply differently to traditional PII than to personal data associated only with a unique identifier. For example, data security is important for all personal data, regardless of type. In contrast, access and correction rights make little sense where a service provider cannot be sure that the user seeking access is the data subject, such as when the data consists of unauthenticated search query logs. For additional discussion of this concept, the Commission may be interested in Victoria Hordern's detailed discussion of different data and data use contexts in her February 2010 article on "Finding Space for a Third Category of Data" located in the BNA International World Data Protection Report.

C. Development of innovative privacy solutions

The report presents an appropriate opportunity for the Commission to adopt a framework that offers guidance on consumer privacy while maintaining flexibility for industry to adapt those principles to various contexts and data channels. The Commission's experience in pursuing problematic conduct under its existing enforcement and regulatory authority provides it with key insights to formulate principles that can guide industry self-regulation and competition on privacy.

The Commission, for instance, actively encouraged industry to take the lead on IBA in its Staff Report on Self-Regulatory Principles for Online Behavioral Advertising released in February of 2009. Shortly thereafter, in March 2009, Google launched its first IBA product with a number of groundbreaking privacy features in place. Other significant IBA industry efforts are also well underway in response to the Commission's urging that industry engage in voluntary efforts to provide protections to consumers. While not a perfect process, self-regulation has created significant progress in advertising privacy over the last several years.

Vibrant competition in the marketplace has also produced a wide array of company-specific privacy-protection options. For example, while we are proud of the privacy features of our search services, some engine providers openly compete with Google on privacy. There are also a large and growing group of privacy tools, including browser plug-ins, that are available to enable users to delete cookies, block online tracking, and opt-out of online ad networks to varying degrees. Indeed, venture funding such as the $7 million recently provided by Steve Case and others, has spotted a market demand for privacy protection technology and is flowing to privacy-related startups.

We encourage the Commission to provide flexibility in its comprehensive privacy framework for such innovative industry efforts to continue.

* * *

We thank the Commission for the opportunity to provide comments on its preliminary privacy report. Please do not hesitate to contact me with any questions by email at pablochavez@google.com or by phone at 202.346.1237.

Sincerely,

Pablo L. Chavez
Director of Public Policy
Google Inc.