



April 14, 2010

Mr. Donald S. Clark
Federal Trade Commission
Office of the Secretary
Room H-135 (Annex P2)
600 Pennsylvania Avenue, NW
Washington, DC 20580
Email Address: privacyroundtable@ftc.gov

VIA EMAIL DELIVERY

Re: Privacy Roundtables – Comment, Project No. P095416

Dear Mr. Clark:

Google would like to thank the Federal Trade Commission for organizing and hosting its recent “Exploring Privacy” roundtable series and for the opportunity to participate in two of the sessions. The roundtables facilitated critical discussions among consumers, industry, advocacy groups, and academics about challenging privacy issues in the increasingly rich Internet environment. The roundtables also laid an important foundation for the work ahead.

Google believes that, going forward, consumer privacy protection will require a multi-faceted solution that includes industry commitments, enhanced statutory protections, and – with a critical role for the FTC – global engagement. Specifically, Google supports:

- **Strong industry commitments to ensure transparency, user control, and security in Internet services for consumers.** Self-regulatory standards, such as the recent work done in online behavioral advertising, have encouraged companies to innovate in the area of privacy and have enhanced user choices in the environment as a whole.
- **Comprehensive privacy standards and strengthened protections from government intrusion.** Google has long supported comprehensive federal privacy legislation to establish baseline privacy protections for consumers. In addition, Google recently announced its support for the reform of federal law governing government access to online records as part of the Digital Due Process coalition (www.digitaldueprocess.org).
- **FTC leadership in the shaping of global privacy standards.** The FTC, in conjunction with the Commerce Department and other stakeholders, has a unique opportunity to develop a workable set of global privacy standards that are comprehensive, flexible, and

effective. The current patchwork of rules and enforcement across multiple jurisdictions does not provide adequate protection for consumers or sufficient certainty for companies offering services on the global Internet.

We offer these points at a critical inflection point for the Internet. Below, we first discuss some of the ways in which privacy and security manifest at Google. We then suggest some considerations for the Commission as it moves forward. We hope our contributions at the roundtables and our comments below are helpful to the Commission in its ongoing effort to steer a course for privacy in the modern economy.

Google's approach to privacy

To give context for our discussion below, we first discuss how Google thinks about privacy internally. Google's motto for product development is "focus on the user and all else will follow." Google has been a leader in developing user-friendly tools to inform and empower our users, including data portability (www.dataliberation.org), educational videos (www.youtube.com/user/googleprivacy), an Ads Preferences Manager that allows users to see and control what interests are associated with their browser (www.google.com/ads/preferences), persistent opt-out cookies (www.google.com/ads/preferences/html/opt-out.html), and a centralized "dashboard" designed to allow users to access their information (www.google.com/dashboard). As Alma Whitten, Google's lead privacy engineer, [recently wrote](#), 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."

These types of privacy tools educate and empower consumers, provide enhanced transparency, and offer meaningful choice without constraining innovation through rigid standards. Our approach aims to serve the privacy interests of our users as well as our collective interest in maintaining an open, innovation-friendly environment that will continue to drive the U.S. economy for years to come.

On International Data Privacy Day 2010, building on our existing privacy framework, we announced our privacy principles, intended to guide our efforts in pursuit of innovation that respects user privacy. In brief, these guiding principles are: (1) use information to provide our users with valuable products and services, (2) develop products that reflect strong privacy standards and practices, (3) make the collection of personal information transparent, (4) give users meaningful choices to protect their privacy, and (5) be a responsible steward of the information we hold. The principles are located at www.google.com/corporate/privacy_principles.html.

In our experience, designing for transparency and user control in a product is critical in the fluid Internet environment. Making progress requires insight into dynamic user needs and nimbleness to respond quickly to user criticism. At Google, we strive to do this across the range of our products. In fact, in just the last year, we sought to tackle three broad privacy issues that face our industry: (a) transparency and choice in the online advertising ecosystem, (b) easy data portability for cloud-based services, and (c) a comprehensive and useful dashboard of privacy controls for a suite of disparate web services.

Transparency and choice for interest-based advertising

In March 2009, Google launched its first interest-based advertising (IBA) product with a number of groundbreaking privacy features in place. As we [told our users](#):

Many websites, such as news sites and blogs, use Google's AdSense program to show ads on their sites. It's our goal to make these ads as relevant as possible for you. While we often show you ads based on the content of the page you are viewing, we also developed new technology that shows some ads based on interest categories that you might find useful.

Google's interest-based ads contain notice in the actual advertisement indicating that it is a Google ad. The in-ad notice is linked to information about IBA, including our Ads Preferences Manager, which allows users to change the interest categories used to target ads or to opt-out of interest-based advertising altogether.



The image shows a screenshot of a TechCrunch webpage on the left and a Lexus advertisement on the right. The TechCrunch page features a main article titled "Apple Countersues Nokia, Accuses Them Of 'Patent Hold-Up'" with a sub-headline "In a very concise statement, Apple has let the public know that it has today filed a counter suit against Finnish handset maker Nokia". The article is dated December 11, 2009. The page also includes a sidebar with "Active Discussed Posts" and a "CrunchGear Holiday Gift Guide" section. The Lexus advertisement on the right is for "LEXUS OF MT. KISCO" and includes the phone number "(914) 241-3500", the website "www.LexusOfMtKisco.com", and the address "275 Kisco Avenue Mt. Kisco, NY 10549". The ad also features the Lexus logo and a "Ads by Google" notice at the bottom.

With our launch of the Ads Preferences Manager (www.google.com/ads/preferences), Google became the first major industry player to empower users to review and edit the interest categories that are associated with their browsers. The Ads Preferences Manager enables a user to see the interest categories Google associates with the cookie stored on her browser, to add interest categories that are relevant to her, and to delete any interest categories that do not apply or that she does not wish to be associated with. Google does not serve interest-based ads based on sensitive interest categories such as health status or categories relating to children under 13.

The Ads Preference Manager also permits users to opt out of interest-based ads altogether. Google implements this opt-out preference by setting an opt-out cookie that has the text "OPTOUT" where a unique cookie ID would otherwise be set. And Google's engineers also developed tools to make our opt-out cookie permanent, even when users clear other cookies from their browser (see

www.google.com/ads/preferences/plugin/). We are encouraged that others are using the open-source code for this plug-in, released by Google, to create their own persistent opt-out tools.



Make the ads you see on the web more interesting

Many websites, such as news sites and blogs, partner with us to show ads on their sites. To see ads that are more related to your interests, edit the interest categories below, which are based on sites you have recently visited.

[Learn more](#)

Your interests are associated with an advertising cookie that's stored in your browser. If you don't want us to store your interests, you can opt out below.

Watch our video:

[Ads Preferences explained](#)



Ads Preferences affect ads that Google shows on other websites.

Your interests	Below you can edit the interests that Google has associated with your cookie:												
<table><thead><tr><th>Category</th><th></th></tr></thead><tbody><tr><td>News & Current Events</td><td>Remove</td></tr><tr><td>Sports</td><td>Remove</td></tr><tr><td>Sports - Basketball</td><td>Remove</td></tr><tr><td>Sports - Soccer</td><td>Remove</td></tr><tr><td>Travel</td><td>Remove</td></tr></tbody></table>		Category		News & Current Events	Remove	Sports	Remove	Sports - Basketball	Remove	Sports - Soccer	Remove	Travel	Remove
Category													
News & Current Events	Remove												
Sports	Remove												
Sports - Basketball	Remove												
Sports - Soccer	Remove												
Travel	Remove												
<div>Add interests</div> Google does not associate sensitive interest categories with your ads preferences.													
Opt out	Opt out if you prefer ads not to be based on the interest categories above. <div>Opt out</div> When you opt out, Google disables this cookie and no longer associates interest categories with your browser.												
Your cookie	Google stores the following information in a cookie to associate your ads preferences with the browser you are currently using: <div><code>id=22586aa4f0000056 t=1252991153 et=730 cs=h5cwyoqd</code></div> Visit the Advertising and Privacy page of our Privacy Center to learn more.												

We have recently begun to get information about how users are interacting with the ad preferences manager. While our data is preliminary, we have noted that for every user that has opted out, about four change their interest categories and remain opted in, and about ten do nothing. We take from this that online users appreciate transparency and control, and become more comfortable with data collection and use when they feel it happens on their terms and in full view.

Data portability

Providing our users with control over their personal information must also mean giving them the ability to easily take data with them if they decide to leave. Starting with our Gmail service and now covering more than 25 Google products where users create and store personal information, a cadre of Google engineers – self-named the “Data Liberation Front” – has built tools to allow our users to “liberate” data if they choose to switch providers or to stop using one of our services. The critical insight of the Data Liberation Front engineers was to recognize that users should never have to use a service unless they are able to retrieve the content they created, get it out easily and for no more than they’re already paying for the service.

Every user of Gmail, Picasa, Reader, YouTube, Calendar, Apps for Business, Docs, iGoogle, Maps, and many other products already have access to data portability tools, and the team continues to work on additional products and services. Detailed information for users is available at www.data liberation.org.

data liberation

Search this site

- ▼ The Data Liberation Front
 - FAQ
- ▼ Google Products
 - AdWords
 - Alerts
 - Analytics
 - App Engine
 - Apps for Business
 - Blogger
 - Bookmarks
 - Calendar
 - Chrome Bookmarks
 - Contacts
 - Docs
 - Finance
 - Gmail
 - Health
 - iGoogle
 - Maps
 - Notebook
 - Orkut
 - Picasa Web Albums
 - Project Hosting
 - Reader
 - Sites
 - Voice
 - Web History
 - YouTube

We intend for this site to be a central location for information on how to move your data in and out of Google products. Welcome.

The Data Liberation Front

The Data Liberation Front is an engineering team at Google whose singular goal is to make it easier for users to move their data in and out of Google products. We do this because we believe that you should be able to export any data that you create in (or import into) a product. We help and consult other engineering teams within Google on how to "liberate" their products. This is our mission statement:

Users should be able to control the data they store in any of Google's products. Our team's goal is to make it easier for them to move data in and out.

People usually don't look to see if they can get their data out of a product until they decide one day that they want to leave. For this reason, we always encourage people to ask these three questions **before** starting to use a product that will store their data:

1. Can I get my data out at all?
2. How much is it going to cost to get my data out?
3. How much of my time is it going to take to get my data out?

The ideal answers to these questions are:

1. Yes.
2. Nothing more than I'm already paying.
3. As little as possible.

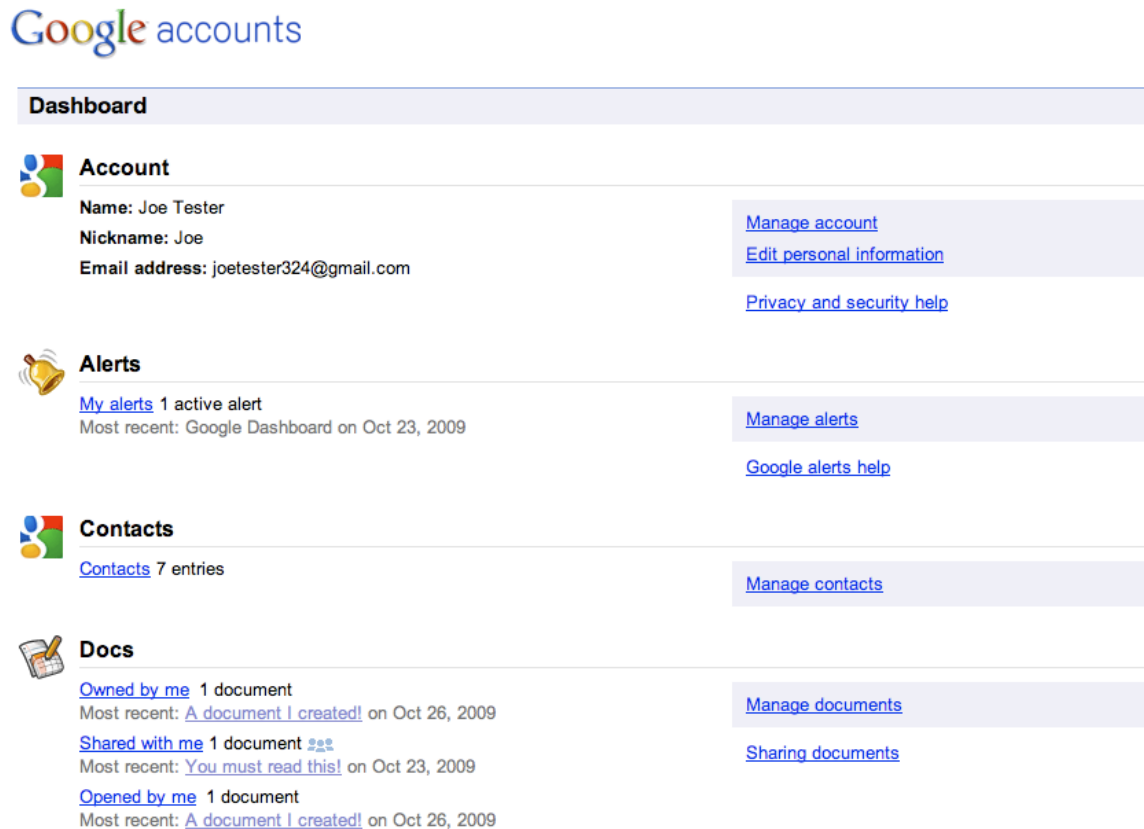
Data portability has benefits for our users and for Google. First, our product teams know just how easy it is for their users to move to a competitor's product, and understand that their success depends upon continuing to be responsive to privacy and product concerns and acting quickly to address them. Second, allowing our users the freedom to leave honors our commitment to put users in control.

In considering the input received by the privacy roundtables and refining its approach to consumer privacy, Google urges the Commission to consider the role that data portability can play in ensuring that consumer facing businesses remain accountable for their privacy choices. The FTC should encourage this kind of "user empowerment by design" as an effective means of ensuring respect for user privacy without chilling innovation.

The Google Dashboard

Google developed the Google Dashboard (www.google.com/dashboard) to provide users with a one-stop, easy-to-use control panel to manage the use and storage of personal information associated with their Google accounts. With the Dashboard, a user can see and edit the personally identifiable data stored with her individual Google account. A user also can change her password or password recovery options using Dashboard, and click to manage various products' settings,

contacts stored with the account, or documents created or stored through Google Docs. Dashboard also lets a user manage chat data, by choosing whether or not to save it in her Gmail account.



The screenshot shows the Google accounts Dashboard for a user named Joe Tester. The dashboard is organized into four main sections: Account, Alerts, Contacts, and Docs. Each section displays a list of items (e.g., documents, alerts) and provides links to manage them. The Account section shows the user's name, nickname, and email address, along with links to manage the account, edit personal information, and view privacy and security help. The Alerts section shows one active alert for the Google Dashboard on Oct 23, 2009, with a link to manage alerts and Google alerts help. The Contacts section shows 7 entries and a link to manage contacts. The Docs section shows documents owned by, shared with, and opened by the user, with links to manage and share documents.

Google accounts

Dashboard

Account

Name: Joe Tester
Nickname: Joe
Email address: joetester324@gmail.com

[Manage account](#)
[Edit personal information](#)
[Privacy and security help](#)

Alerts

[My alerts](#) 1 active alert
Most recent: Google Dashboard on Oct 23, 2009

[Manage alerts](#)
[Google alerts help](#)


Contacts

[Contacts](#) 7 entries

[Manage contacts](#)

Docs

[Owned by me](#) 1 document
Most recent: [A document I created!](#) on Oct 26, 2009

[Shared with me](#) 1 document 
Most recent: [You must read this!](#) on Oct 23, 2009

[Opened by me](#) 1 document
Most recent: [A document I created!](#) on Oct 26, 2009

[Manage documents](#)
[Sharing documents](#)

Providing stewardship through security

Along with transparency and user control, security plays an important role in maintaining user trust. Google faces complex security challenges while providing services to millions of people every day. We have a world-class team of engineers dedicated to helping secure information, who work regularly with our product managers and engineers to provide design reviews, security consulting, and training and education about security issues.


Security is at the core of our design and development process. For example, Google recently became the first major webmail provider to offer session-wide SSL encryption by default. And last month Google launched a system to notify users about suspicious activities associated with their accounts. By automatically matching a user's IP address to broad geographical locations, Google can help detect anomalous behavior, such as a log-in appearing to come from one continent only a few hours after the same account holder logged in from a different continent. Thus, someone whose Gmail account may have been hijacked will be notified and given the opportunity to change her password, protecting her own account and her Gmail contacts.

Similarly, we built Google Chrome with security in mind from the beginning, including features such as:

- Safe Browsing, which warns a user before he visits a site that is suspected of phishing or containing malware;
- Sandboxing, which helps prevent web browser processes from harming one another or a user's computer, and
- Automatic updates that deliver security patches to users as quickly as possible.

Google also conducts extensive security research and provides free security resources to the broader Internet community. We make security tools available for free to webmasters to help them operate more secure sites, as well as to application developers to help them build more secure applications. For example, we [recently released](#) a tool called “skipfish” under an open source license to help identify web application vulnerabilities through fully automated, active security reconnaissance.

[My favorites ▼](#) | [Sign in](#)


code skipfish
web application security scanner

Search projects

Project Home
Downloads
Wiki
Issues
Source

Summary
Updates
People

skipfish

A fully automated, active web application security reconnaissance tool. Key features:

- **High speed:** pure C code, highly optimized HTTP handling, minimal CPU footprint - easily achieving 2000 requests per second with responsive targets.
- **Ease of use:** heuristics to support a variety of quirky web frameworks and mixed-technology sites, with automatic learning capabilities, on-the-fly wordlist creation, and form autocompletion.
- **Cutting-edge security logic:** high quality, low false positive, differential security checks, capable of spotting a range of subtle flaws, including blind injection vectors.


The tool is believed to support Linux, FreeBSD 7.0+, MacOS X, and Windows (Cygwin) environments.

Quick links:

- [Download current version](#) (1.31 beta)
- [See detailed documentation](#)
- [View a sample screenshot](#)


Troubleshooting tips:

- [Check the list of known problems](#) (and workarounds)
- [File a bug in the tracker](#)

Activity:  [High](#)

Code license:
[Apache License 2.0](#)

Labels:
[security](#), [web](#), [scanner](#), [http](#), [google](#)

Featured downloads:
 [skipfish-1.31b.tgz](#)
[Show all »](#)

Featured wiki pages:
[SkipfishDoc](#)
[Show all »](#)

Feeds:
[Project feeds](#)

Owners:
[Icamluf](#)
[People details »](#)

Policy recommendations

Google is encouraged to see the deep commitment of the FTC to privacy, as represented by its thoughtful approach to these roundtables. As we learned at the roundtables, there is much to be proud of in terms of existing U.S. consumer privacy protections: Congress has set important rules governing data collection, use, and security in many sectors, and the FTC and states have used their general consumer protection authority to protect privacy. Responsible businesses, with guidance from government and advocates, have developed self-regulatory codes that reflect respect for user privacy and security. Moreover, this has been accomplished in ways that have not inhibited innovation and growth in the Internet economy.

We also continue to believe that the principles of transparency and user control are of foundational importance in the existing privacy environment and should continue to be at the core of privacy. While we recognize that traditional fair information practice principles (FIPPs) may need to be

updated, Google is concerned about proposals to discard the notice and choice paradigm altogether. Notice and choice – where “notice” is robust and easy-to-understand and choices are empowering and meaningful – remains a powerful model for the protection of privacy. Moreover, it allows important decisions about product functionality and data uses to remain in the hands of consumers.

We also learned in the roundtables some important lessons about how industry and regulators can improve on the existing framework and adapt it to changing use patterns and conditions. Ensuring adequate privacy and continued innovation will require new ideas and renewed effort.

The role for industry self-regulatory principles

We believe that there is an important role for the development and enforcement of industry self-regulatory privacy principles – especially for business models and industries that are inherently fast-moving and innovative. Combining principles with a baseline uniform legislative foundation, discussed below, ensures accountability to consumers for privacy practices. This approach also preserves companies’ incentive to innovate, because it reduces the fear that unintentional missteps will result in disproportionate penalties.

Thus, for example, we agree with the Commission’s conclusion that self-regulation is the preferred approach for online interest-based advertising, and we support the FTC’s efforts to push the industry toward enacting meaningful and enforceable standards in this area. We are also encouraged by recent work by the Interactive Advertising Bureau, Network Advertising Initiative, and others to develop self-regulatory principles for online behavioral advertising. Such self-regulatory efforts could be helpful in other areas of the online ecosystem as well, as they can be developed and adopted in pace with technology and usage.

Updating privacy laws for the global Internet

Google supports the passage of a comprehensive federal privacy law that would accomplish several goals, including:

- Building consumer trust;
- Establishing a baseline set of privacy principles, on which self-regulatory efforts could build;
- Establishing a uniform framework for privacy, which would create consistent levels of privacy from one jurisdiction to another; and
- Enacting penalties to deter bad behavior and punish bad actors.

In addition to a baseline standard for transparency and user control, a comprehensive privacy law should include uniform data safeguarding standards, data breach notification procedures, and stronger procedural protections relating to third party access to individuals’ information.

As information flows increase, and more and more information is processed and stored in the Internet “cloud,” there is a greater need for consistency and trust over the security of online data.

In this vein, stemming from our support for stronger procedural protections relating to government access to information, Google is an active member of Digital Due Process (www.digitaldueprocess.org), a coalition of online businesses, electronic communications services

providers, and leading civil liberties organizations seeking modest but critical reform of federal laws relating to the privacy of electronic communications.

The changes recommended by the coalition are necessary to assure that users of cloud computing services are protected against unreasonable searches and seizures of digital content, and to ensure that U.S. providers of such services can compete effectively with offshore providers. The FTC, too, should encourage the Administration and Congress to update the Electronic Communications Privacy Act to ensure consistent government standards for online consumers. As a law enforcement agency with direct experience in obtaining access to individuals' personal information in connection with investigations, the FTC could play an important part in ensuring adequate and coherent reform.

International engagement

Though getting privacy right in the domestic context is critical, this task cannot take place in a vacuum. It is essential that U.S. policy makers take into account – and meaningfully engage in – the international effort to develop and harmonize data protection policy. This is especially true given the importance of the Internet to the world economy.

The wisdom gained through the roundtables offer useful insight into consumer privacy protection as international privacy organizations and regulators revisit the FIPPs. The Commission, along with the Commerce Department and other U.S. representatives, should make full use of the opportunity to influence the global privacy regulatory debate. We support the Commission's active participation in international discussions with this goal in mind.

Maintaining a regulatory environment that encourages responsible privacy practices while also promoting continued Internet innovation will require the leadership of broad-minded, forward-looking U.S. regulators, including the FTC. The international regulatory patchwork makes it increasingly hard for companies to operate internationally, even while commerce is becoming increasingly global. United States leadership in creating a uniform, flexible, and comprehensive approach to privacy protection that effectively educates users, vests them with meaningful control, and earns their trust could help remove artificial barriers to the free flow of information.

Free expression and privacy

Google acts every day to promote and expand free expression online and increase global access to information. As new technology empowers individuals with more robust free expression tools and greater access to information, we believe that governments, companies, and individuals must work together to protect the right to online free expression.

Strong privacy protections must be crafted with attention to the critical role privacy plays in free expression. The ability to access information anonymously or pseudonymously online has enabled people around the world to view and create controversial content without fear of censorship or retribution by repressive regimes or disapproving neighbors. While we cabin this right in important ways – including individual liability for defamation or harmful speech – it is invaluable to the ability to exercise freedom of expression.

As the Web evolves, free expression can also be affected by mandated opt-in policies for information collection. While appropriate in certain circumstances, broad opt-in requirements can

create perverse incentives for companies to collect more identifying information than necessary and to obtain “consent” in inappropriate or confusing ways. If all online behavior were traced to an authenticated identity, the free expression afforded by anonymous web surfing would be jeopardized.

Conclusion

Google wishes to thank the FTC for considering these comments as it contemplates its future efforts to protect the privacy of consumer data. We hope that our privacy efforts, as described here, can inform those efforts and help in the Commission in its daunting task. Google will continue working with the FTC to think deeply about the acceptable treatment of user data both across jurisdictions and across the private and public spheres.

Should you wish to contact us regarding our comments, please do not hesitate to contact me by email at pablochavez@google.com or by phone at 202.346.1237.

Sincerely,

Pablo L. Chavez
Managing Policy Counsel
Google Inc.