Google Inc.
76 Ninth Avenue
4th Floor
New York, NY 10011

Google

Main 212 565-0000
Fax 212 565-0001
www.google.com

November 26, 2008

Consumer Watchdog
Jamie Court, President
John M. Simpson, Stem Cell Project Director
1750 Ocean Park Blvd, #200
Santa Monica, CA 90405

Dear Mr. Court and Mr. Simpson:

Thank you for your letter dated October 13, 2008 regarding our new Google Chrome browser, and for taking the time to discuss that letter with us in a subsequent phone meeting. As discussed during our phone conversation of October 20, we welcome input from privacy and consumer advocates regarding our products, and we are always looking for ways in which we can better serve our users.

In our quickly evolving business environment, ensuring that we earn and keep our users' trust is an essential constant for 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' information. The bedrock of our privacy practices are three design fundamentals: providing transparency, choice, and security.

Another constant that we have found in our business is that innovation is a critical part of protecting privacy. To best innovate in privacy, we take the feedback of privacy advocates, government experts, our users, and other stakeholders. While we very much welcome your input, we believe that in several instances you may have misunderstood our products and practices. During our phone call, we had an opportunity to discuss your video (http://www.youtube.com/watch?v=ncerhCLi2o0) regarding the Google Chrome browser and its "Suggest" feature. The video makes several inaccurate statements regarding our privacy practices with respect to the Suggest feature and incognito mode. Below, we clarify how Google Chrome works:

- ***Our Suggest feature protects user privacy***. At several points, the video claims that Google is storing every keystroke associated with the Suggest feature, and in a manner associated with the user (such as through IP address). As discussed on our call, this is not the case. Google stores a random sample of only 2% of requests received through Suggest in order to monitor and improve the service. To protect user privacy, we anonymize the IP addresses within 24 hours of receiving this random sample. Additionally, users can turn off the Suggest feature at any time by clicking the wrench

icon, going to the "Options" menu and clicking the "Manage" button on the "Basics" tab. To learn more about how Google Suggest works, please view our blog (http://googleblog.blogspot.com/2008/09/update-to-google-suggest.html).

- ***Google does not facilitate packet sniffing.*** A significant part of your privacy concerns centers on the possibility of interception through packet sniffing. The type of interception you warn against is, fortunately, nearly impossible on the open Internet, and is also illegal under federal and state laws. Additionally, your concerns about packet sniffing do not take into account the distributed design of the Internet, where most traffic takes many different routes to a destination. Moreover, such interception is a remote risk, given the small number of entities with the ability to access a user's activity. These concerns are about the behavior of bad actors or a few companies, such as Internet Service Providers (ISPs), that are in a position to look at all of a user's web activity, whether at home or at work. We would also like to point out that the risk of misconduct by ISPs applies to all of a user's Internet activity (including Internet banking, email, or other activity far more sensitive than search) and not exclusively to Google's Suggest feature, as your video implies.

- ***Incognito mode protects privacy on users' computers and limits data collection by third parties.*** Incognito mode is a privacy-enhancing feature we built into Google Chrome to help users surf the Internet without leaving information on their own computers about the sites they've visited. Every time users open an incognito mode window, they are given a prominent notice regarding what the feature does and does not do. For example, the pages you view in incognito mode do not leave cookies on your computer and will not appear in your browser history or search history. Incognito mode does not default to Secure Socket Layer (SSL) connections because these connections are provided by websites, not browsers, so it is technologically impossible for Google Chrome to behave this way. To learn more about privacy while using Google Chrome, you can watch a video in the Google Privacy Channel on YouTube (http://www.youtube.com/watch?v=pWk8uGdUEkQ).

- ***We continue to improve Google Chrome for the benefit of our users.*** Although your video accurately points out a bug in our initial implementation of incognito mode, where some data is sent to Google when the user experiences a navigational error, we have corrected the issue so that such data is no longer sent, and we thank you for calling it to our attention.

We also received your letter dated November 17, 2008, and have viewed the video (http://www.youtube.com/watch?v=dg7pVFVqMMg) showing your further concerns about Google Chrome and about Gmail. As with your first video, we believe that you may have misunderstood our products and practices. Below, we clarify how our products function:

- ***Google Chrome Shortcuts is an opt-in feature.*** The desktop feature for Google Chrome Shortcuts is designed for users who affirmatively choose to use it, so that the user can access the website as if it is an application without the distraction of the navigation

buttons. Users who prefer to see full navigation buttons can open the application in Google Chrome normally. In order for the desktop application to exist, the user must proactively create the desktop application from a website. It does not happen by default or accidentally.

- ***SSL and SafeBrowsing work for all versions of Google Chrome.*** Both SSL and SafeBrowsing work normally when Google Chrome is in desktop application mode. However, the fact that both features continue to function normally in this mode is not fully transparent to users because the gold lock icon indicating that they have an SSL connection does not appear. This is an area where we could make improvement, and we will take your recommendation into consideration.

- ***Gmail leads the industry in protecting web email.*** Gmail has supported SSL from the day it launched, even though other free webmail services typically do not support SSL. SSL keeps mail encrypted as it travels between your web browser and our servers. We use SSL to protect your password every time you log into Gmail, but we don't use SSL once you're in your mail unless you ask for it. This is because SSL can make your mail slower. Your computer has to do extra work to decrypt all that data, and encrypted data doesn't travel across the Internet as efficiently as unencrypted data, particularly on mobile devices.

- ***We provide features such as auto-save in Gmail for a better user experience, while at the same time giving users options for additional security measures.*** Gmail users have almost universally expressed appreciation for our auto-save feature, which helps users maintain their message drafts in the cloud in case of a browser crash. Additionally, users can access Gmail more securely over https at any time by clicking on "Settings" at the top of any Gmail page and setting "Browser Connection" to "Always use https." Accessing Gmail over https makes drafts virtually impenetrable to snooping. We leave the choice to use it by default up to the user because, as noted above, encrypted data can make your mail slower.

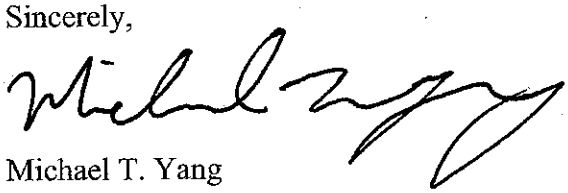
- ***Users choose how to send and receive their email messages.*** Your video suggests that Gmail may compromise the privacy of those who send email messages to Gmail accounts, since the senders have not necessarily agreed to Google's privacy policy or Terms of Service. This is based on a misunderstanding of how Gmail works. In any email exchange, senders and recipients have the option to determine how messages are respectively sent and retrieved, as well as what email service provider they may choose to use. Just as senders have the option to decide to whom to send messages, and to choose an email provider that they trust to deliver those messages, recipients of email messages have the option to read their email messages in any way they choose. With Gmail, no one other than recipients is allowed to read the email messages they receive, and no one other than recipients sees contextual ads and related information. We believe that many users will choose Gmail over other services, with full knowledge that Gmail is supported by advertising, and with confidence that Google is protecting the privacy of all of their email messages.

- ***Advertising on Gmail is done in a privacy-friendly way.*** Virtually all email services scan your email to provide such popular features as spam filtering, virus detection, search, spellchecking, and the automatic saving and sorting into folders. Google also uses this scanning technology to deliver relevant text ads and other related information. This is completely automated and involves no human review. It is important to note that the ads in Gmail are dynamically generated each time a message is opened by the user. In other words, Google does not attach particular ads to individual messages or to users' accounts.

Although we have several disagreements with some of the claims made in your videos and letters, we are always open to suggestions on how to meaningfully improve user privacy in our products. Regarding Google Chrome specifically, we are still collecting user feedback during our beta period and will review it with some of your suggestions in mind. We will also take some of your broader suggestions under consideration. In the meantime, we invite you to review our Privacy Center (http://www.google.com/privacy) where we provide more information about our privacy practices.

We appreciate your continuing interest in protecting consumer privacy, and we welcome your efforts to learn more about the privacy protections that Google offers its users and the practices of the Internet industry more generally.

Sincerely,



Michael T. Yang
Senior Product Counsel
Google Inc.