



Formerly The Foundation for Taxpayer & Consumer Rights

1750 Ocean Park Boulevard, #200, Santa Monica, CA 90405-4938 • Tel: 310-392-0522 • Fax: 310-392-8874 • www.consumerwatchdog.org

October 13, 2008

Eric Schmidt
Chairman and Chief Executive

John Doerr
Director

Sergey Brin
Co-founder & President

Ram Shriram
Director

Larry Page
Co-Founder & President, Products

John L. Hennessy
Director

Arthur Levinson
Director

Paul S. Otellini
Director

Shirley M. Tilghman
Director

Ann Mather
Director

Google Inc.
1600 Amphitheatre Parkway
Mountain View, CA
94043

Dear Directors,

We are writing you with serious privacy concerns about Google's browser Chrome, Chrome's "Incognito Mode," and the asynchronous communication of personal data through many of Google's products and services without appropriate transparency and control for users. Consumers using your products are in an unnoticed conversation with Google as the company collects user data on its servers. This is unacceptable and one of the reasons why Consumer Watchdog was forced last week to write the Justice Department in opposition to your proposed advertising alliance with Yahoo. (Read our letter at <http://www.consumerwatchdog.org/resources/JusticeGooglelet100208.pdf>).

Google has offered many products and services that are extremely useful and highly valued by consumers. Precisely because you have been so successful with your search engine, functions like Gmail, Google Maps and Chrome, Google has unprecedented dominance over the transmission of computer data. Your dominant market position demands higher privacy standards and protections; you should be the gold standard for the industry.

Before the introduction of the Chrome browser, Google was the world leader in search and web analytics. Google received data, aggregated it and analyzed it for companies, advertisers and websites that paid handsomely, as well as for individuals who received customized information and services. Google was primarily on the outside looking in. But with Chrome's release, Google is now also on the inside sending information out. With this software inside individuals' computers, Google's role as sender *and* receiver of data has become uniquely powerful and threatening to the privacy of users.

The danger is that Google – the original Google that sells analytical, or detailed web usage services – has such a financial interest in knowing ever more about who we are and what we say and do online that the beachhead it has established with Chrome might leave no room for user privacy whatsoever.

The introduction of Chrome, unless the privacy concerns are addressed seriously and quickly, could mark the end of real user control and choice online because:

(1) New asynchronous communications are occurring without users' full understanding, consent or control;

(2) Many Chrome features blur the distinction between the desktop and Internet-based cloud computing, where a computer user's software, documents, data and personal information exist not on the consumer's hard drive but on Google's servers on the Internet. This creates confusion in the consumer's mind about the privacy and security of confidential information;

(3) Chrome's Incognito mode lulls consumers into a false sense of security that their actions are completely private and free from prying eyes when in fact they are not.

Chrome is the keystone that bridged a tolerable separation between desktop and cloud computing. With Chrome, the distinction between what is on our computers and what is on your servers is being phased out. Now, Google has the onus to create facilities that allow consumers to easily and clearly choose between the two worlds, rather than be forced to be a prisoner of Google's Web.

The chart below shows Google's unparalleled dominance on the Internet in this unique sender/receiver role. As the chart shows, Google is the only major Internet company that controls a web analytics enterprise and has a browser with asynchronous communications, yet Google does not offer transparency or easy opt-out for these communications. Google must adjust its privacy model for greater transparency, disclosure, ease of use and user control of the information that they share with Google.

				 Apple	 Mozilla
Major Web Analytics Business	YES Market Leader	NO Minor System	YES	NO	NO
Browser	YES Chrome	YES Internet Explorer	NO	YES Safari	YES Firefox
Major Search Engine	YES Market Leader	YES MSN & Live.com	YES	NO	NO Google Deal
Asynchronous <i>Auto-Suggest</i> In Address Bar	YES	NO	N/A	NO	NO
Software Triggers communication with Company	YES	NO	YES	NO	NO
Hidden & Difficult To Opt Out of <i>Auto-Suggest</i> in Search Engine	YES	N/A	NO	N/A	YES Google Engine

The Chrome tool bar’s suggestion function (like the Google Search engine’s suggestion function) fundamentally alters the typical request-response pattern of the Internet. By merely typing, without clicking “Search” on either the tool bar or the search engine, a user in Google’s default mode has shared information with Google through an unnoticed conversation between computers. This asynchronous acquisition of user information appears innocuous and helpful to most Chrome and Google Search engine patrons, who do not mentally link the auto suggest feature to the fact that Google is spying on every keystroke, not just every search.

Even for users who seek out and use “Incognito” mode, some information is shared with Google. As we discuss below, “Incognito” is not really incognito.

To illustrate Chrome’s privacy risks for Internet users, Consumer Watchdog has begun posting a series of videos about Google’s practices on <http://www.consumerwatchdog.org/google> and <http://www.googlespy.org>

The asynchronous search suggestion function in Chrome’s address bar is not a function in other browsers. Internet Explorer, Safari and Firefox do provide address bar suggestions but the browser only uses personal search history on the user’s computer. Chrome’s address bar communications with Google servers expands the reach of the asynchronous auto suggest function of Google.com’s search engine. Yahoo’s search engine also has an auto suggest function, but it is fairly well disclosed and easily turned off, as opposed to Google’s, which requires leaving the search page itself and knowing where to look.

We ask that Google offer on its search engine page and other products a simple, conveniently located “anonymizer” button (or perhaps you’ll call it “Incognito Mode” to

follow the new Chrome feature) that can be clicked on and off. We also request more accessible information and transparency about features that passively acquire information. Google's unique new Internet role as databank and data transmitter via Chrome requires this type of attention to privacy.

Chrome's "Incognito Mode" does protect a user from leaving information about visited sites on the computer. This kind of privacy is important when multiple users share a computer. However, the name "Incognito" lulls many users into believing it provides more privacy than is the case, as our first video begins to demonstrate. Quite simply, despite users' reasonable belief that they can surf the web anonymously when they select Incognito, Chrome continues to send some information back to Google and allows data collection tied directly to the user's computer. When someone selects Incognito mode, we assume, and Google should too, that the user doesn't want anyone watching or having a record of their computing. But, as it is currently configured, Chrome allows users to be incognito to some people, while exposed to others (namely Google).

You should provide the privacy the name implies or stop calling it Incognito mode.

Consumer Watchdog is calling for three important changes to Chrome and the Google websites.

- Google should place a single prominent button on the main Chrome interface that can't be hidden or removed and that allows a user to enter Incognito mode instantly without interrupting the user experience. Once in Incognito mode, the application should assume we want to stay incognito, essentially treating Incognito as a default preference once a user has selected it.
- Google should provide clear disclosure on the Google search engine home pages so that users can easily prevent communication with Google before pressing the search button or affirmatively requesting an action. This could be an extension of an omnipresent "Incognito mode" button. This disclosure needs to be made clear throughout all the Google applications including Gmail, Google Talk, and the Google Toolbar. This disclosure needs to be more than a confusing warning a few clicks away. It should be a convenient, actionable feature so that the user can exercise informed choice.
- Incognito should have the full meaning the word implies when users opt for it. Incognito mode should default to SSL (Secure Socket Layer) connections, provide an automatic IP anonymizing service, enforce a no-log policy on all Google servers including Google Analytics, as well as disable auto-saving, suggestions, and all other features that use asynchronous event handlers other than button and link click. Incognito should disable all external calls to desktop applications and plug-ins whose applications fail to meet equivalent standards.

Finally, Google should publish these standards so other software vendors and websites can develop based on a new Chrome Incognito Privacy standard that ensures consumer privacy not just throughout the Google network but throughout the Web itself.

Chrome represents a once-in-a decade opportunity to raise the consumer privacy bar to new heights that will benefit consumers, content providers, and ultimately Google itself.

We look forward to your response and to working with Google to make the company the standard bearer for privacy on the Internet.

Sincerely,

Jamie Court

John Simpson