Searching for Privacy: How to Protect Your Search Activity

Abstract: This guide explains how to perform searches anonymously, protecting you from increasingly intrusive tracking and analysis by corporate and governmental organizations.

Toll free: 866.760.0222
Toll free: 0808.101.2678
www.ioactive.com

IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

Contents

Understanding the Problem

> *If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place. If you really need that kind of privacy, the reality is that search engines—including Google—do retain this information for some time and it's important, for example, that we are all subject in the United States to the Patriot Act and it is possible that all that information could be made available to the authorities.*
> *—Eric Schmidt, CEO of Google*

Every computer-based search that involves your putting data into an internet search engine subjects you to having that term—along with discernable information about you including your ISP, your search history, potentially even your name and address—stored and provided to advertisers, search marketers, and law enforcement entities. You won't be notified when this happens and you certainly won't be asked for your consent beforehand.

Every time you perform a search for something, that information is cached and linked to you as an entity. If you perform a search on your name, social security number, or credit card data (even if it's just out of curiosity), you have effectively given away control of that information and it's now available for distribution. There's a lot of data about us available on the Internet and there are few who would willingly have it sold without their approval. Every day we lose more control over our personally identifiable information (PII) and no one knows exactly how Google (and others) are securing it.

You are not Anonymous

When you browse the web and conduct searches, there are two primary means by which you can be identified:

- The internet connection you are using has a network IP address associated with it, which can be tracked over time and linked back to a provider and perhaps location.
- Web sites send uniquely generated identifiers (cookies) to your web browser that are stored and referenced on future visits, allowing activity over time to be linked to a single user.

These means of identification allow correlation and analysis of search records to form a view of your identity that you may not wish to expose.

In early 2005, the United States Department of Justice filed a motion in federal court to force Google to comply with a subpoena for, "*the text of each search string entered onto Google's search engine over a two-month period (absent any information identifying the person who entered such query).*" Google fought the subpoena over concerns about users' privacy. In March 2006, the court ruled partially in Google's favor, recognizing the privacy implications of turning over search terms and refusing to grant access.

On August 4, 2006, AOL put a file on one of its websites for research purposes that caused a public relations nightmare. The contents of that file included 20 million search keywords for over 650,000 of its users with the result that—while not always identifiable by name—users were identified with little effort due to their ego-searching activities. Users had typed in their own names, addresses, and even social security numbers, and the New York Times was able to locate one individual by doing a phone book cross reference.

Then, in May 2010, more wood was thrown on the fire when Google disclosed that it had collected personal data sent over public WiFi networks (including unencrypted search requests) while gathering street-view images for its mapping service. This was followed on May 21 by their releasing an encrypted version of Google Search that utilizes SSL to secure its core search functionality, but not the Images or Maps features.

Still, this move does little to address the anonymization issue. According to Google's privacy FAQ, *"Google anonymizes its IP data after nine months and its cookies after 18 months."* What this means is that that your unanonymized data can be sold for 9–18 months after it's been generated.

A Solution

Figure 1 shows an implementation stack available to any standard PC that allows bypass of identification mechanisms and obtains a higher level of anonymity:

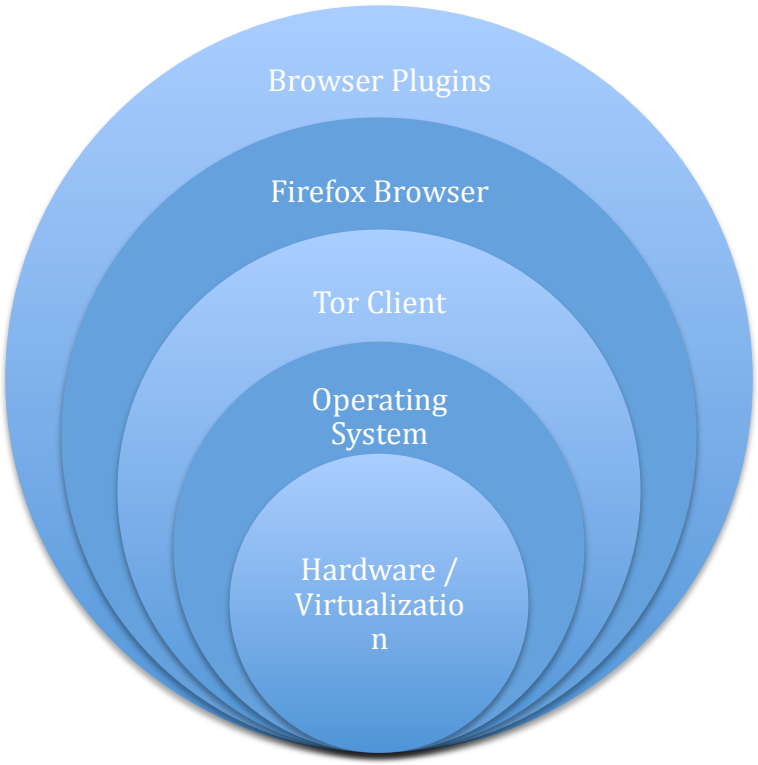


Figure 1: Anonymous browsing technology stack

The stack components include:

- **Hardware / Virtualization.** This solution will work inside of your existing hardware or—for additional protection—you may wish to create a separate virtualized environment using a product such as VMWare or VirtualBox.
- **Operating System.** Any operating system that is supported by a Tor client and Firefox browser (see below) may be used including Windows XP/Vista/7, Mac OS X, Linux, and others.
- **Tor Client.** Tor offers protection by bouncing your communications through a distributed network of relays run by volunteers all around the world. It prevents anyone who is watching your Internet connection from learning what sites you visit and it prevents the sites you visit from learning your physical location.
- **Firefox Browser.** A free web browser that is available for download from *getfirefox.com*. Configured with cookies, but with JavaScript, Java, and Flash disabled.
- **Browser Plugins.** Torbutton, CustomizeGoogle, and Scroogle SSL are Firefox plugins that can be combined to achieve ongoing anonymity.

The next section walks you through the steps of implementing this system and configuring your computer to perform searches anonymously.

Configuring your computer to perform anonymized searches

1. Working on the system that you want to anonymize (personal computer or virtualized system), download and install Tor, available from: <http://www.torproject.org/download.html.en>

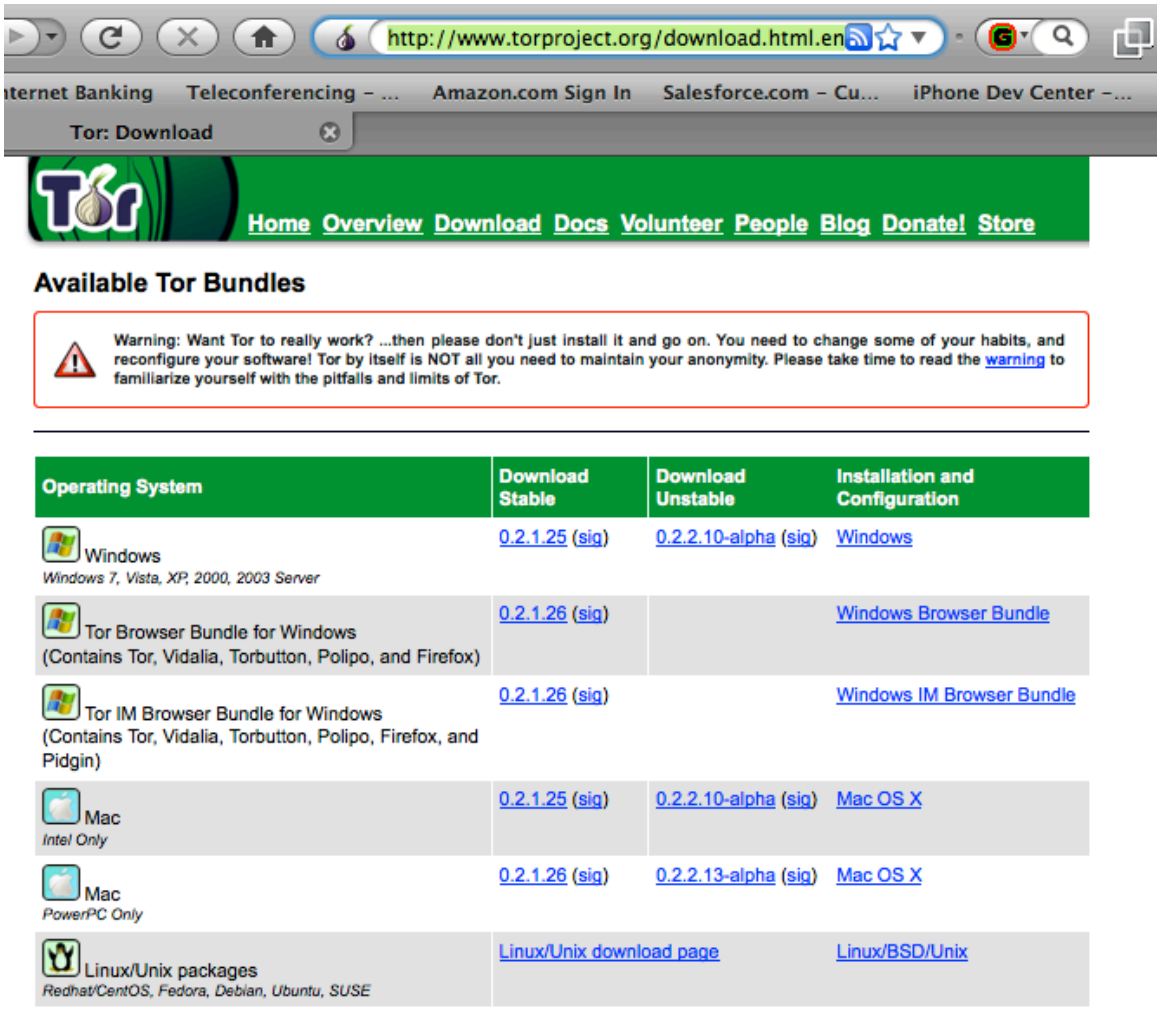


Figure 2

2. Start the Tor client.

3. Using the Firefox browser, install and start the Torbutton plugin: in the lower right-hand corner of the browser window, click **Tor Disabled**.

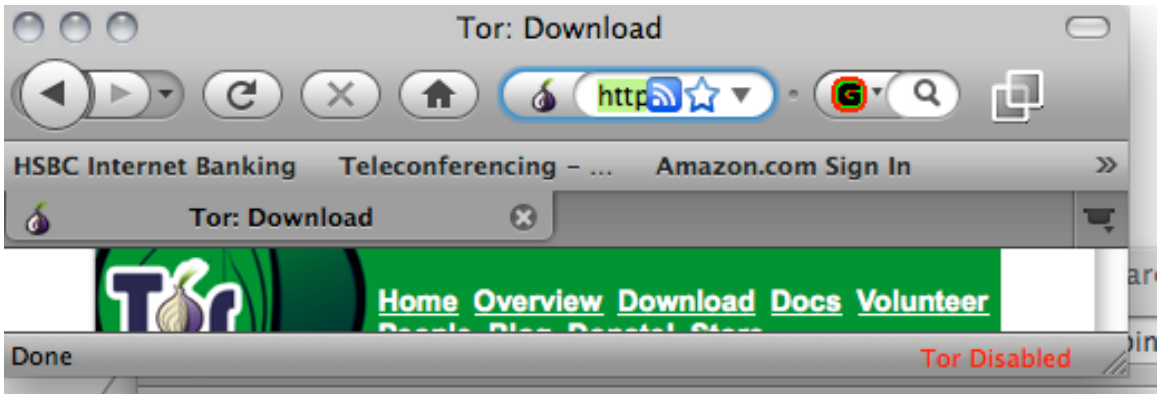


Figure 3: Tor disabled

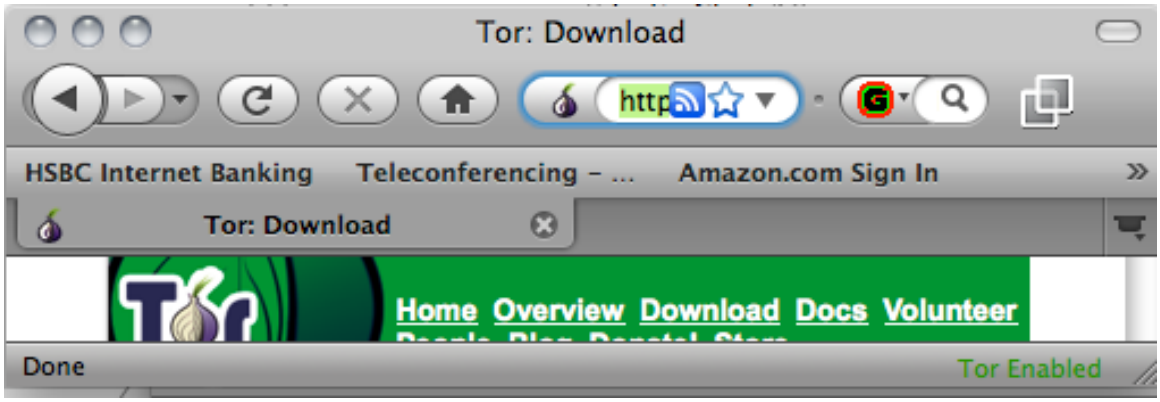


Figure 4: Tor enabled

4. Using the Firefox browser, download and install the CustomizeGoogle plug-in, available from: <http://www.customizegoogle.com>.

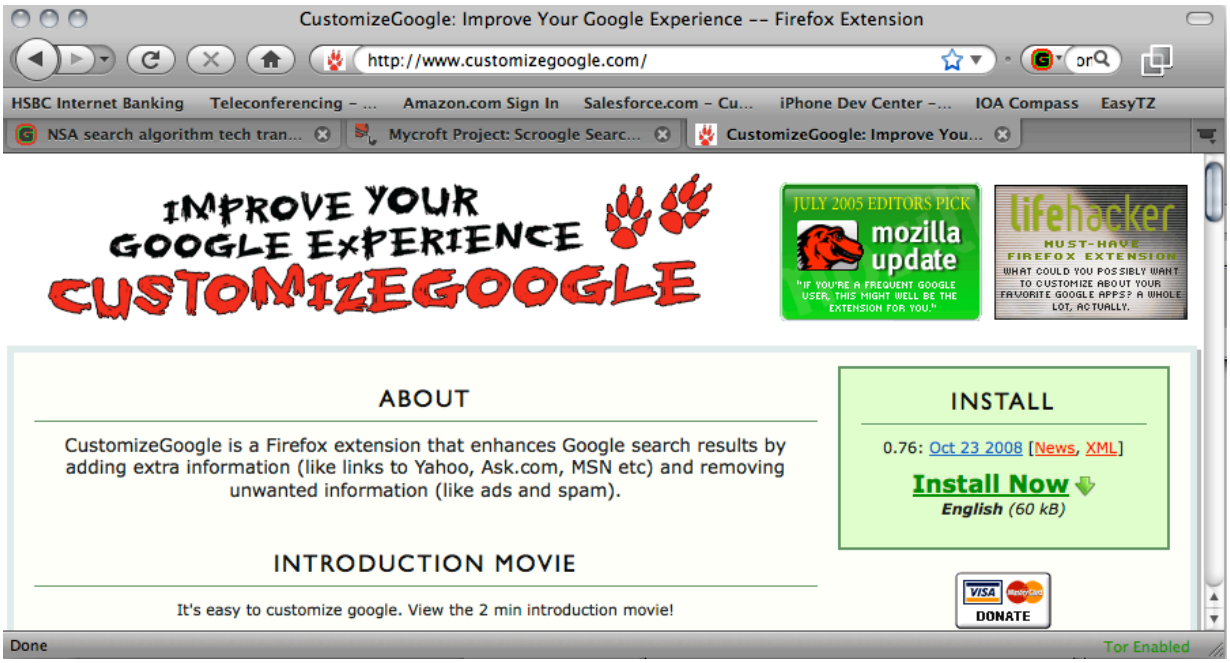


Figure 5

5. In CustomizeGoogle, under the **Web** menu, select the **Remove click tracking** checkbox, as shown in Figure 6.

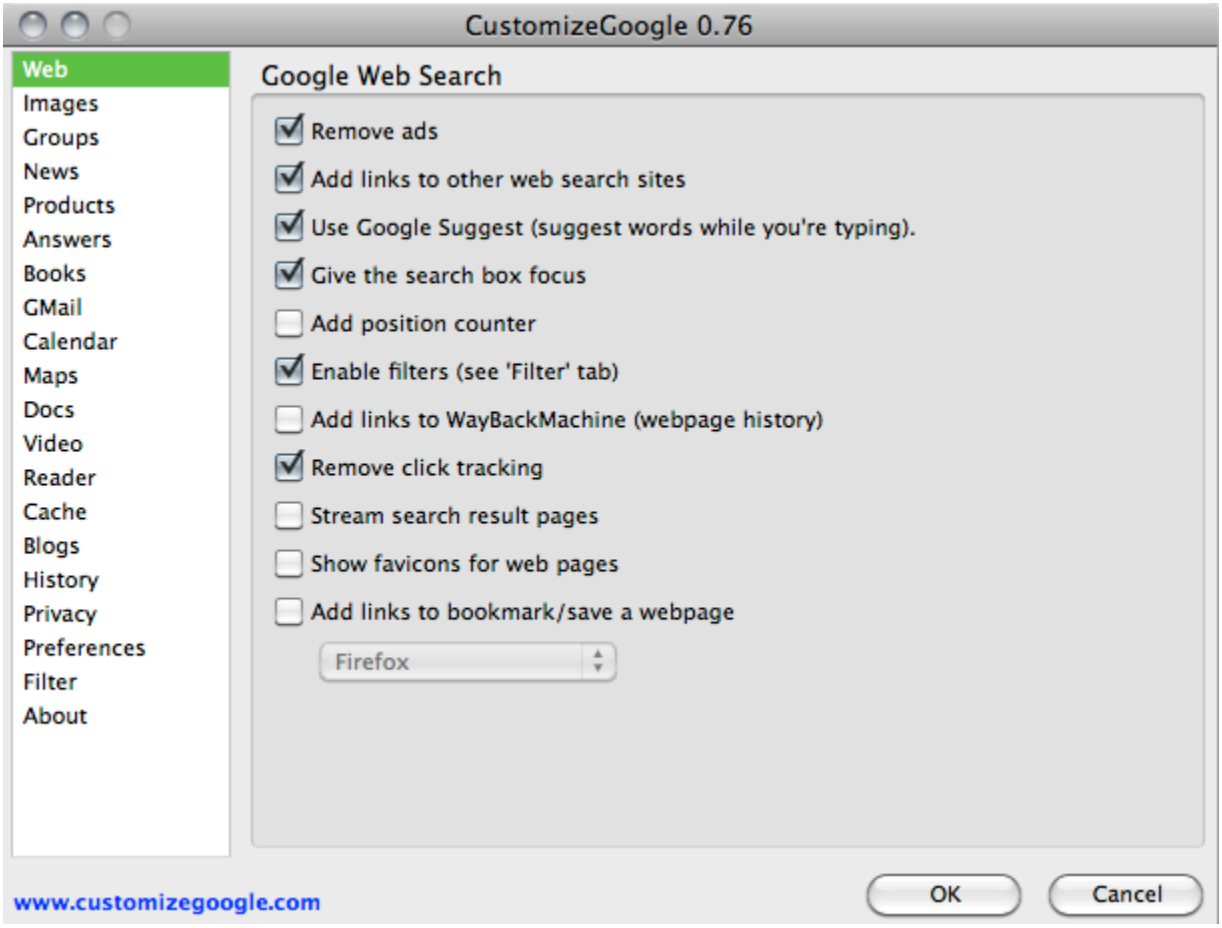
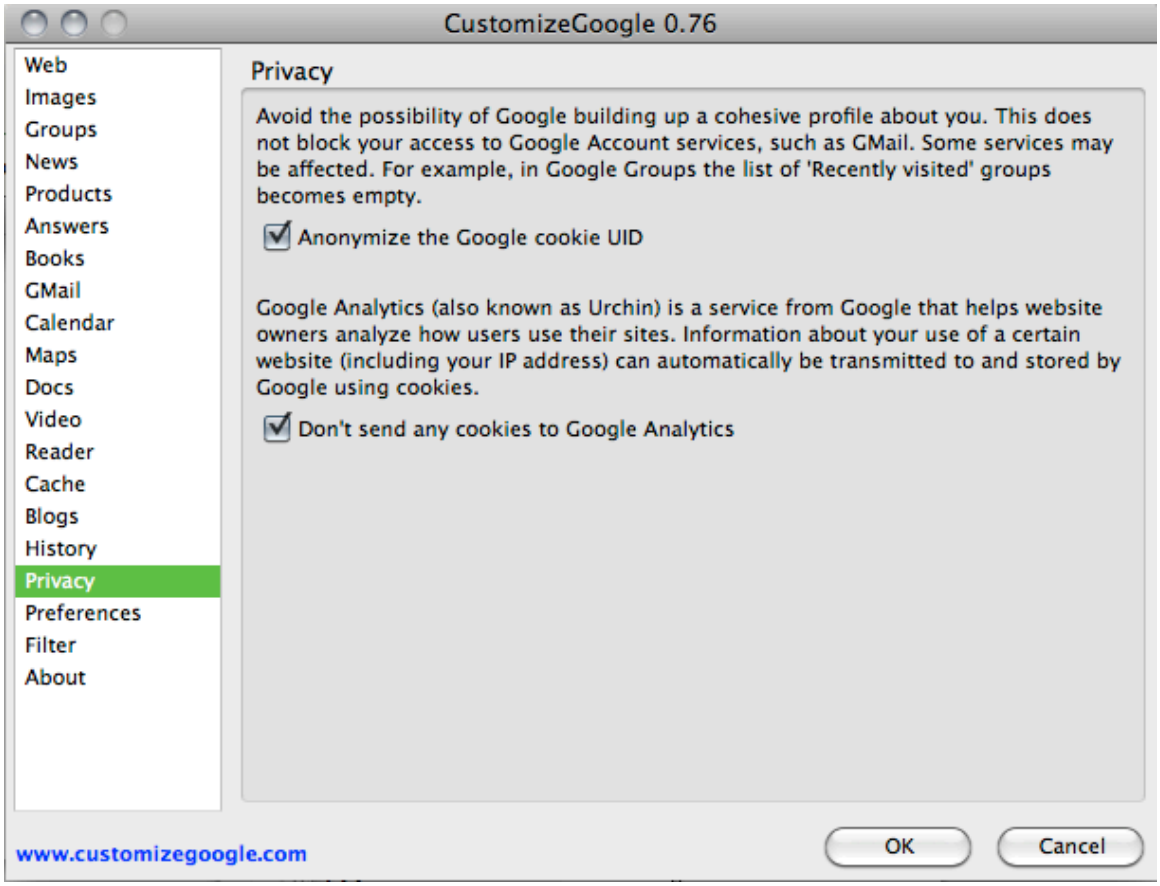
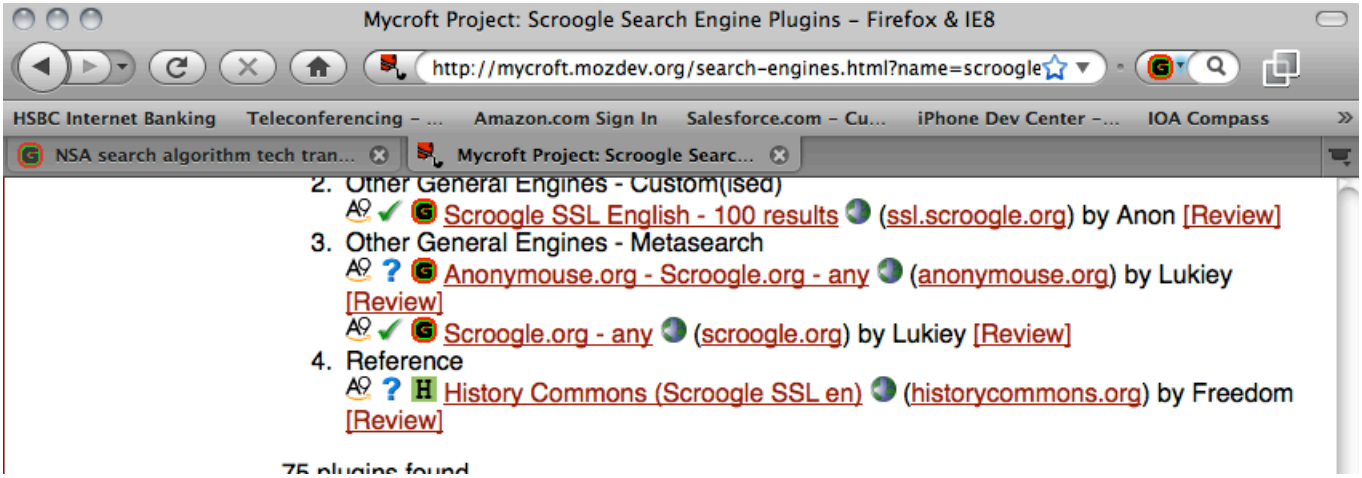


Figure 6

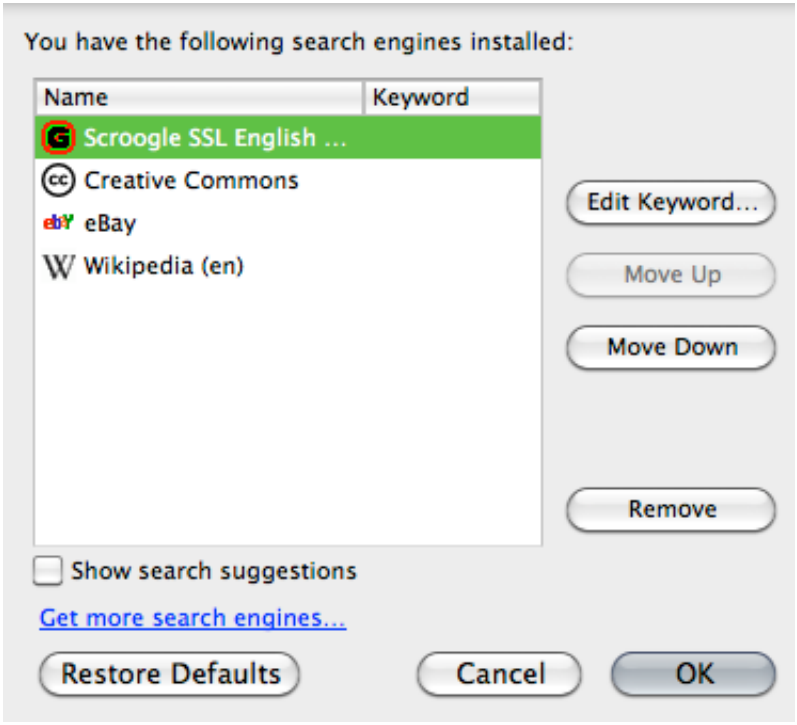
6. In CustomizeGoogle, under the **Privacy** menu, enable cookie mangling by selecting the **Anonymize the Google cookie UID** and **Don't send any cookies to Google Analytics** checkboxes.



7. Using the Firefox browser, download and install Scroogle SSL, available from: <http://mycroft.mozdev.org/search-engines.html?name=scroogle>



8. Make Scroogle your default search engine by moving it to the top of the stack.



9. Use Scroogle to conduct a search, as shown by the sample in Figure 7, which was conducted over the Tor network; this combination circumvents Tor nodes that monitor egress traffic.

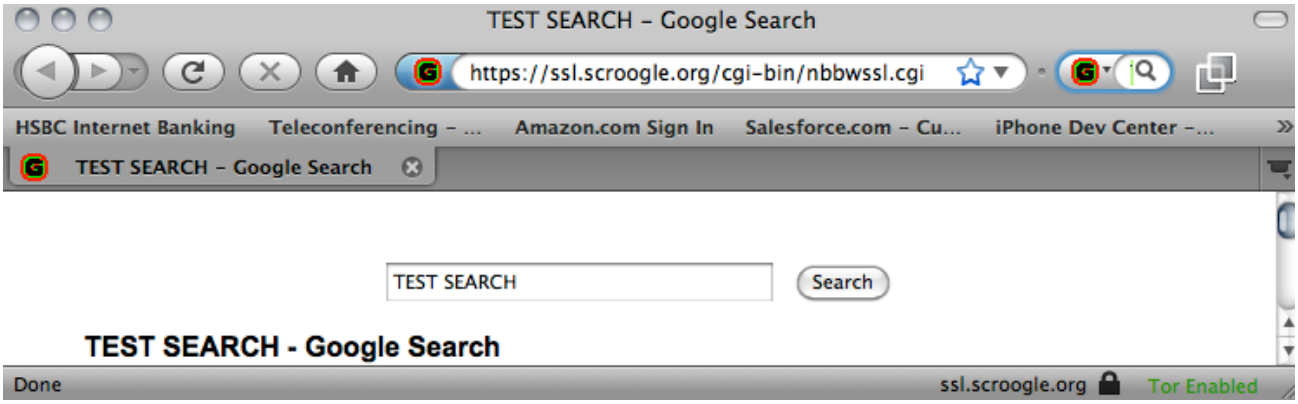
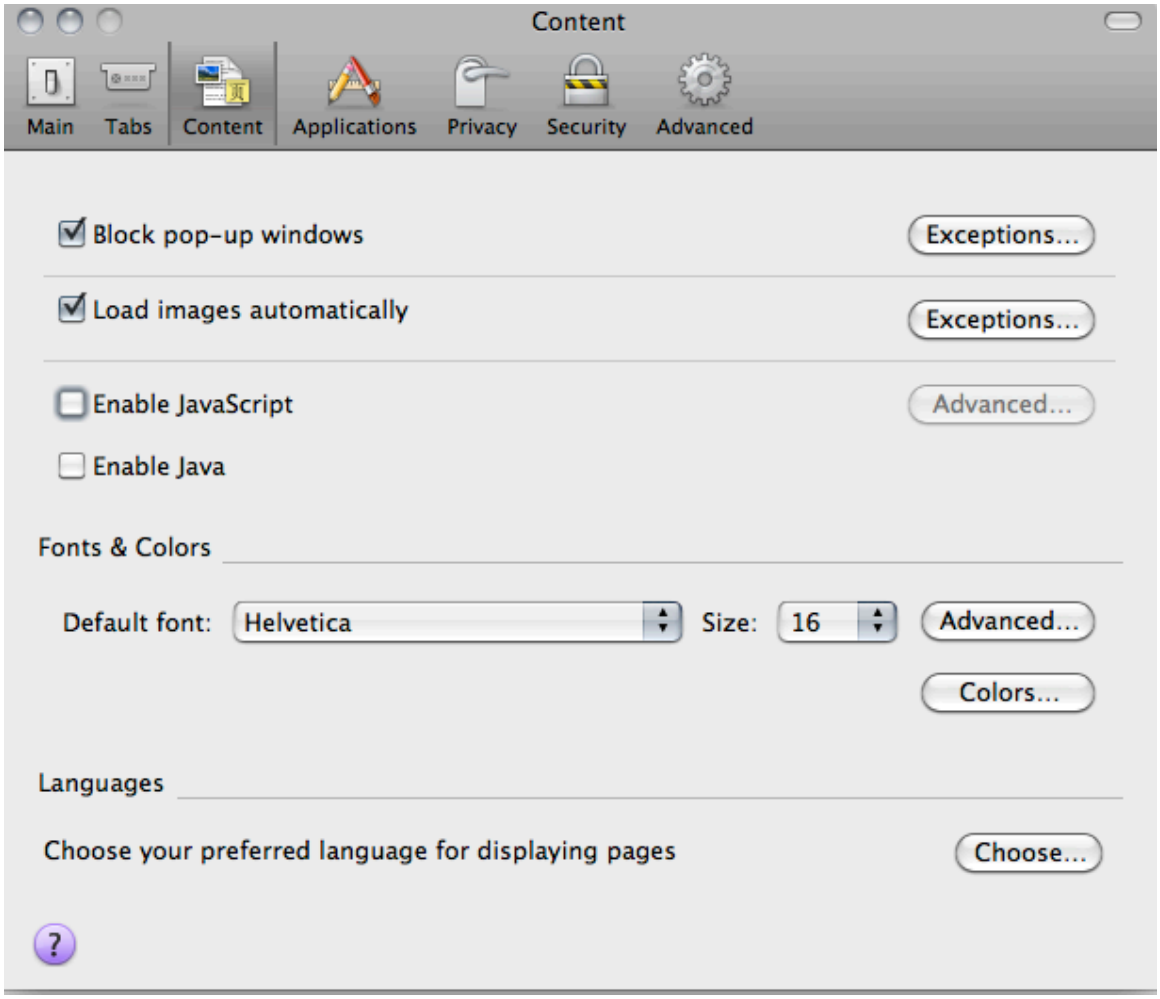


Figure 7

10. In Firefox, on the **Content** menu, de-select the **Enable JavaScript** and **Enable Java** checkboxes.



11. In Firefox, on the **Privacy** menu, ensure that your settings reflect those shown in Figure 8.

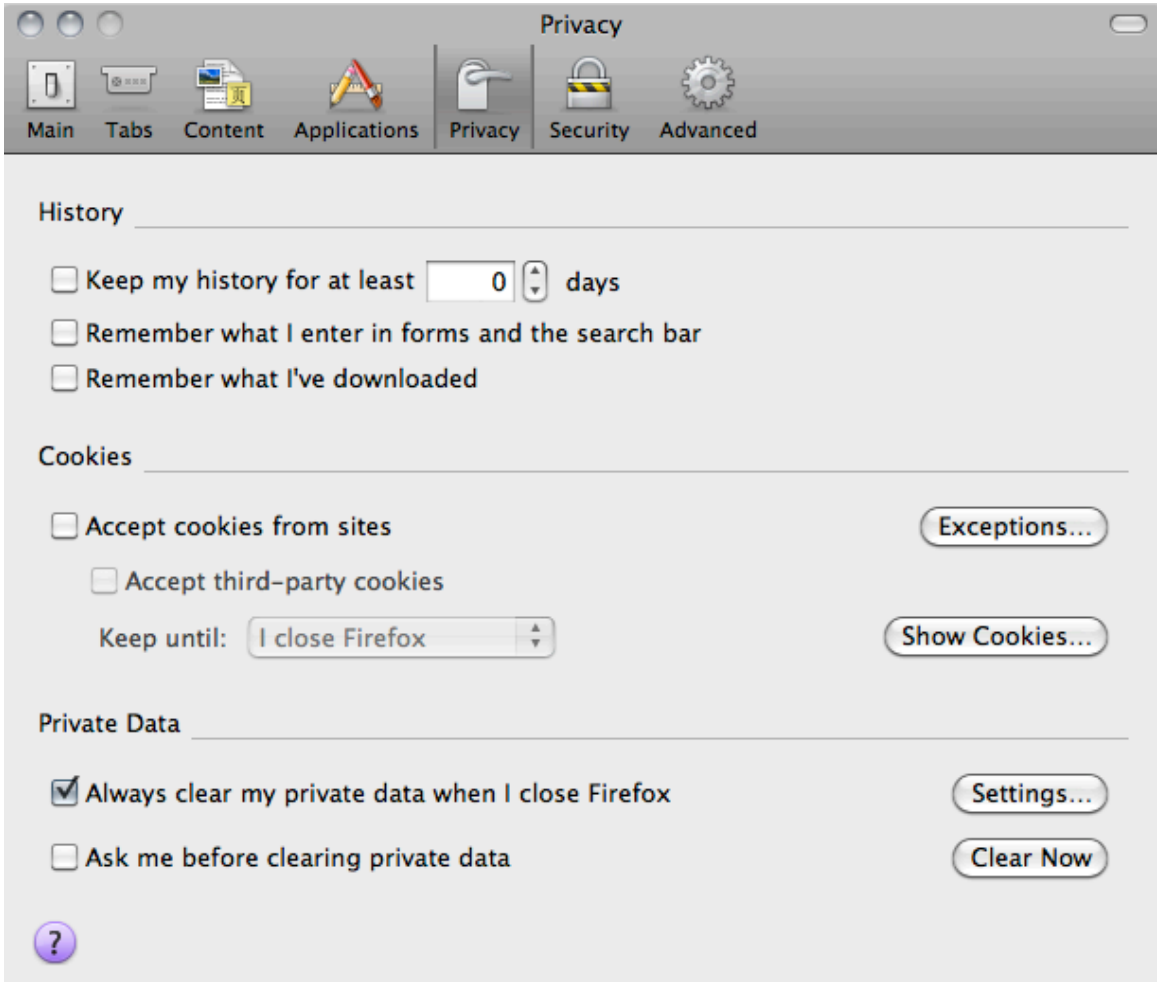


Figure 8

12. In Firefox, from the **Privacy** menu, next to **Always clear my private data when I close Firefox**, click **Settings**. Select all the data types that you wish to be erased, using Figure 9 as a guide.

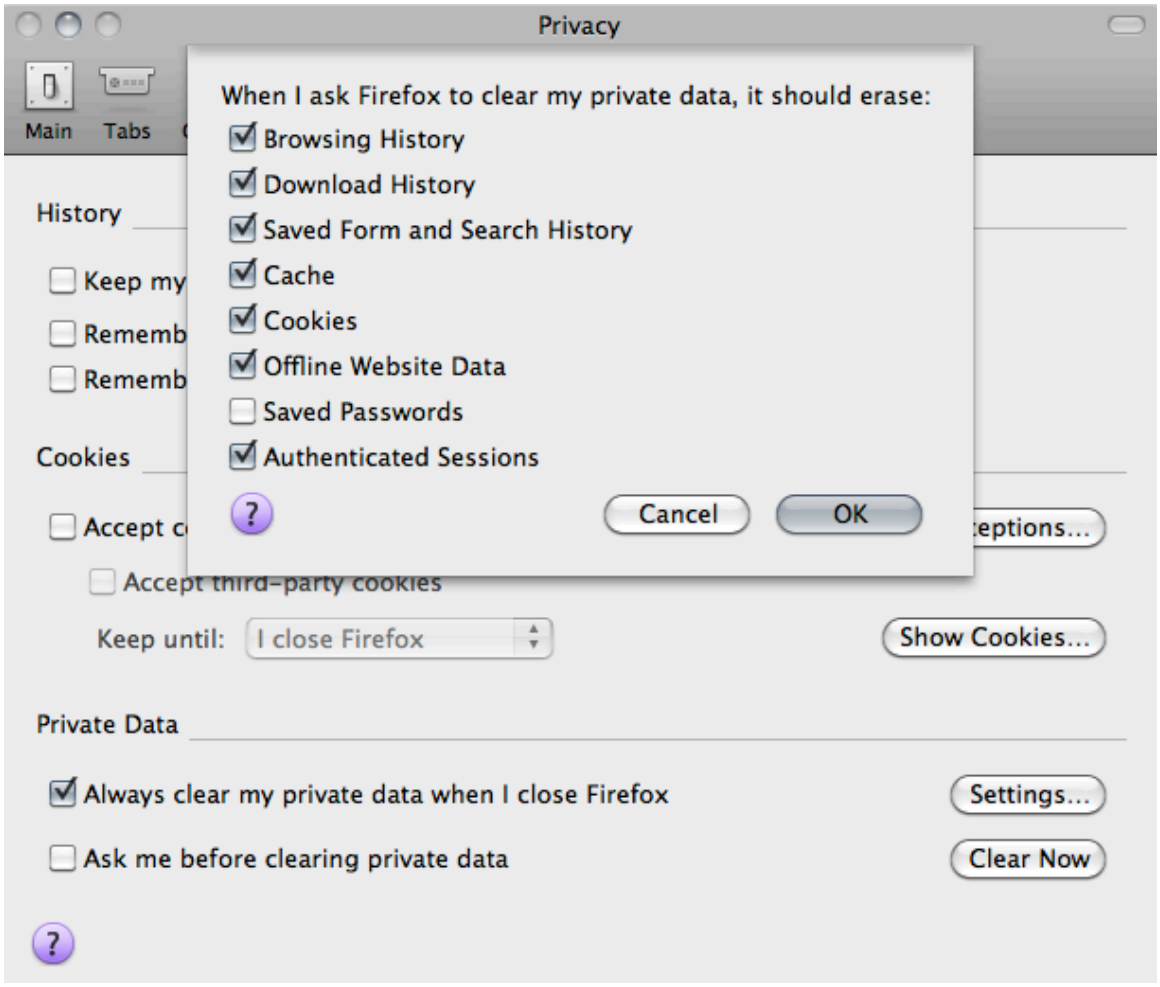


Figure 9

13. In Firefox, from the **Advanced** menu, ensure that your proxy settings look similar to those shown in Figure 10.

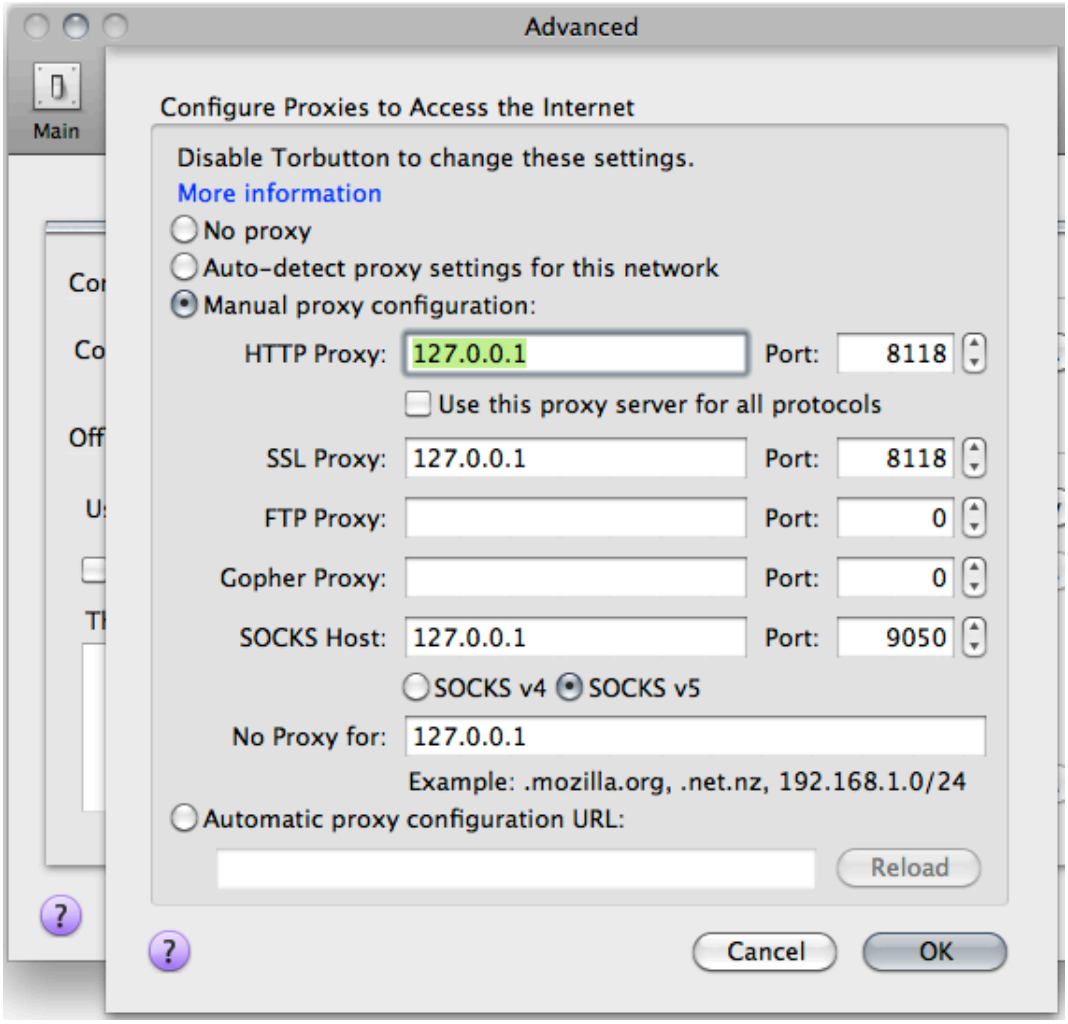


Figure 10

Conclusion

Having completed these steps, you now should be able to browse and search with anonymity. However, it is important to remember that you should never use the anonymous browsing environment to access commonly-used websites where you are required to log in as doing so may compromise your efforts. You may wish to use a separate browser, computer, or virtualized system for this purpose.

This guide has focused on Google as a search provider, but other search providers are likely to have similar capabilities. Even with this anonymization stack in place, there still exist numerous ways in which your personal information can be compromised; the following online resources can help protect you even further.

- http://www.eff.org/wp/six-tips-protect-your-search-privacy

- http://blog.searchenginewatch.com/060123-112156

References

http://www.theregister.co.uk/2010/05/12/scroogle_returns/

http://www.theregister.co.uk/2009/12/07/schmidt_on_privacy/

http://www.imilly.com/google-cookie.htm

About IOActive

Established in 1998, IOActive is an industry leader that offers comprehensive computer security services with specializations in smart grid technologies, software assurance, and compliance. Boasting a well-rounded and diverse clientele, IOActive works with a majority of Global 500 companies including power and utility, hardware, retail, financial, media, router, aerospace, high-tech, and software development organizations. As a home for highly skilled and experienced professionals, IOActive attracts the likes of Dan Kaminsky, Ilja van Sprundel, Mike Davis, and Wes Brown—talented consultants who contribute to the growing body of security knowledge by speaking at such elite conferences as Black Hat, Ruxcon, Defcon, Shakacon, BlueHat, CanSec, and WhatTheHack. For more information, visit www.ioactive.com.