# Browser Privacy Features: A Work In Progress

## August 2009 – Version 2.0

This report reviews and compares the privacy tools available for the latest versions of Mozilla Firefox, Microsoft Internet Explorer, Google Chrome, Apple's Safari, and the Opera Web browser. We compare the browsers in their offering of three key tools -- privacy mode, cookie controls and object controls – which can greatly reduce the amount of personal information users transmit online and leave behind on their computers. This is an update to version 1.0 of this report, which was released in October 2008.

Several of the largest Internet companies have recently released new Web browsers or browser features aimed at giving Internet users greater control over their privacy as they surf the Web. That browser makers are competing to provide the best privacy protections is great news for Internet users, who will hopefully see continuing improvements in the simplicity and accessibility of browser controls that allow them to manage the information they generate and transmit over the Internet.

This 2.0 version of the report updates version 1.0, which was released in October 2008. Version 2.0 compares the privacy features available in five Web browsers – Firefox 3.5, Internet Explorer 8, Google Chrome, Safari 4, and Opera 10. Three types of features are analyzed in the charts below: privacy modes, cookie controls, and object controls. We also evaluate the most popular add-ons for each browser and feature type: CookieSafe for cookie controls in Firefox, AdBlock Plus for object controls in Firefox and PithHelmet for object controls in Safari.[1]

[1] PithHelmet was tested using Safari 3. A PithHelmet version compatible with Safari 4 is not yet available.

**Privacy Mode:** The main motivation behind a browser privacy mode is to allow users to browse without leaving data trails on their computers. In the normal course of Web surfing, browsers record and retain a lot of information locally on users' computers. Browsers save visited Web sites in the browsing history, downloaded files in the download history, and search terms in the search history. Browsers can also save the data typed into online forms (including passwords) and cached versions of files that may be needed again in the near future. The privacy modes in each of the browsers aim to reduce the local storage of these kinds of information, providing increased privacy on shared computers.

**Cookie Controls:** Some kinds of cookies facilitate the tracking of Internet users or store identifying information (or both). Cookie controls allow users to decide which cookies can be stored on their computers and transmitted to Web sites.

**Object Controls:** Increasingly, cookies are not the only tracking mechanism available to Web sites and services. Other kinds of data repeatedly transmitted to or from a user's browser across different sites may also be used to log and profile the user's Web activities. In this report we use the term "object controls" to describe browser mechanisms that allow users to decide which of these other mechanisms to block or allow on their computers.

This report does not address other browser features such as Web search boxes or malware or phishing detection.

Apple, Google, Microsoft, Mozilla and Opera verified the accuracy of the claims made in the report about their browser software.

The browser is the gateway to the Internet for many consumers. Ensuring that browser privacy controls are easy to find and simple to use is one crucial component of empowering consumers to maintain their privacy online. Improvements in this area cannot replace the need for a robust national privacy law, but they go a long way towards putting consumers in control of their own data.

## Privacy Mode Comparison

Many of the browsers provide some sort of privacy browsing mode. This mode is generally aimed at reducing or eliminating the storage of data locally on the user's computer. In some cases, this mode also affects data – specifically, cookies – transmitted by the browser. All of the browsers also have a "clear private data" menu option that achieves similar results to a privacy mode on a single-use basis. All of the privacy mode features are present in each browser's "clear private data" option except for the last three listed in the table below.

| Privacy Mode Comparison | Chrome's Incognito | IE8's InPrivate Browsing | Firefox 3.5's Private Browsing | Safari's Private Browsing[2] | Opera 10 |
|---|---|---|---|---|---|
| Visited sites are not stored in the browser history | ✓ | ✓ | ✓ | ✓ | |
| Downloaded files are not stored in the download history | ✓ | | ✓ | ✓ | |
| Form field data (including passwords) is not stored | ✓ | ✓ | ✓ | ✓ | |
| Addresses typed into the address bar are not stored | ✓ | ✓ | ✓ | ✓ | |
| Visited links are not stored | ✓ | ✓ | ✓ | ✓ | |
| Search queries are not stored in the browser | ✓ | ✓ | ✓ | ✓ | |
| Cached files are deleted at the end of the browsing session | ✓ | ✓ | ✓ | ✓ | |
| Existing third-party cookies cannot be read | ✓ | ✓ | ✓ | ✓ | |

[2] The behavior of Safari was observed on Mac OS X, where Safari is predominately used. Safari behavior on other operating systems may differ.

| Privacy Mode Comparison | Chrome's Incognito | IE8's InPrivate Browsing | Firefox 3.5's Private Browsing | Safari's Private Browsing[2] | Opera 10 |
|---|---|---|---|---|---|
| New cookies are deleted at the end of the session | ✓ | ✓ | ✓ | ✓ | |
| Blocks referring URL from being sent.[3] | | ✓ | | | ✓[4] |
| Mode can operate on a per-window basis. | ✓ | ✓ | | | |
| Mode can persist even when user quits and re-starts browser. | | | | | |

[3] As users navigate from one site to another, a referring URL is often passed along from the previous site, indicating the Web address that the user last visited.

[4] Opera does not have a privacy mode, but has a menu option for this feature.

## Cookie Controls Comparison

In the comparison below, global cookie controls that apply to an entire class of cookies (first-party or third-party) are distinguished from granular cookie controls that users can set on a site-by-site basis.

| Cookie Controls Comparison | Chrome | Internet Explorer 8 | Firefox 3.5 | CookieSafe Firefox Add-On | Safari | Opera |
|---|---|---|---|---|---|---|
| **Global first-party cookie options.** | • Block<br>• Allow | • Block<br>• Allow<br>• Prompt<br>• Allow session cookies<br>• Block or restrict according to automated privacy policy[5] | • Block<br>• Allow<br>• Prompt | • Block<br>• Allow | • Block<br>• Allow | • Block<br>• Allow<br>• Prompt<br>• Delete upon exit |
| **First-party cookie default setting.** | Allowed | Allowed, with cookies restricted according to automated privacy policy | Allowed | Allowed | Allowed | Allowed |

[5] IE8 gives users a number of options to block or restrict cookies with compact P3P policies that allow the sites setting the cookies to contact users with their implicit or explicit consent.

| Cookie Controls Comparison | Chrome | Internet Explorer 8 | Firefox 3.5 | CookieSafe Firefox Add-On | Safari | Opera |
|---|---|---|---|---|---|---|
| **Global third-party cookie options.** | • Restrict: Allow setting but not reading | • Block<br>• Allow<br>• Prompt<br>• Allow session cookies<br>• Block or restrict according to automated privacy policy | • Block<br>• Allow<br>• Prompt | • Block<br>• Allow | • Block | • Block<br>• Prompt<br>• Delete upon exit |
| **Third-party cookie default setting.** | Allowed | Allowed, with cookies blocked according to automated privacy policy | Allowed | Allowed | Blocked | Allowed |
| **Granular (per-site) cookie options.** | None | • Block<br>• Allow<br>• Privacy import option for more specificity[6] | • Block<br>• Allow<br>• Allow only on a session basis | • Block<br>• Allow<br>• Allow for current session<br>• Allow only on a session basis[7] | None | • Block<br>• Allow<br>• Allow only first-party cookies<br>• Allow only on a session basis<br>• Prompt |

[6] IE8 allows users to import an XML privacy preferences file that can describe granular preferences for cookies from particular sites.

[7] CookieSafe allows users to specify that only session cookies should be accepted from a given site. This differs from the option of allowing cookies from a particular site to be set and read only until the user closes the browser (i.e., allowed for the current session).

| Cookie Controls Comparison | Chrome | Internet Explorer 8 | Firefox 3.5 | CookieSafe Firefox Add-On | Safari | Opera |
|---|---|---|---|---|---|---|
| **Cookie retention options.** | None | Privacy import option allows specificity | • Until manually deleted<br>• Until browser is closed<br>• Prompt each time | • Until manually deleted<br>• Until browser is closed<br>• Prompt each time<br>• User-specified retention time | None | • Until manually deleted<br>• Until browser is closed |
| **Blocking cookies from being set prevents existing cookies from being read.** | For first-party cookies, yes. For third-party cookies, 'Restrict' option blocks setting but not reading. | When blocking is set via privacy setting, yes. When blocking is set via advanced controls, no. | Yes | Yes | No | Yes |
| **Can automatically prevent deleted cookies from being reset.** | No | No | No | Yes | No | No |

## Object Controls Comparison

Browsers receive and transmit content of many different types – everything from basic text and images to style sheets, scripts, "Flash cookies" and more. When the same objects appear repeatedly across different sites, they could potentially be used to track Internet users. The comparison below describes browser controls around such objects, plus browser features that can be used to block entire Web sites or domains from communicating with the browser. The ability for users to create lists of objects to block or allow onto their computers is also addressed.

| Object Controls Comparison | Chrome | Internet Explorer 8 | Firefox 3.5 | AdBlock Plus Firefox Add-On | Safari | PithHelmet Safari Add-On | Opera 10 |
|---|---|---|---|---|---|---|---|
| **Automatically blocks some objects.** | No | Yes, with InPrivate Filtering. | No | No | No | Yes | No |
| **Objects blocked:** | | All objects served or requested from unique domains by third parties more than 10 times.[8] | | | | Blocks a selection of ad servers and other domains by default. | |

[8] Subdomains are not considered as separate unique domains and do not increase this count. In addition, the setting can be changed to block objects that have been received from a smaller or larger number of sites.

| Object Controls Comparison | Chrome | Internet Explorer 8 | Firefox 3.5 | AdBlock Plus Firefox Add-On | Safari | PithHelmet Safari Add-On | Opera 10 |
|---|---|---|---|---|---|---|---|
| **Users can manually block individual objects (other than cookies).** | No | Yes, with InPrivate Filtering. | Yes | Yes | No | Yes | Yes[9] |
| **Restrictions on which objects can be blocked:** | | Third party objects that appear on automatically generated list. | Images only | Objects expressible in AdBlock filter language[10] | | Objects expressible in PithHelmet rule editor[11] | Images, Java, Javascript, CSS |
| **Supports block lists.** | No | Yes, with InPrivate Filtering. | No | Yes | No | No | Yes |
| **Supports automatic updating of block lists.** | No | No | No | Yes | No | No | No |

[9] Opera can also block any visible object on a page.

[10] AdBlock Plus supports "filters" that allow users to set rules manually about objects to be blocked or allowed. These rules are expressed in a language that can be interpreted by a user-installed filter.

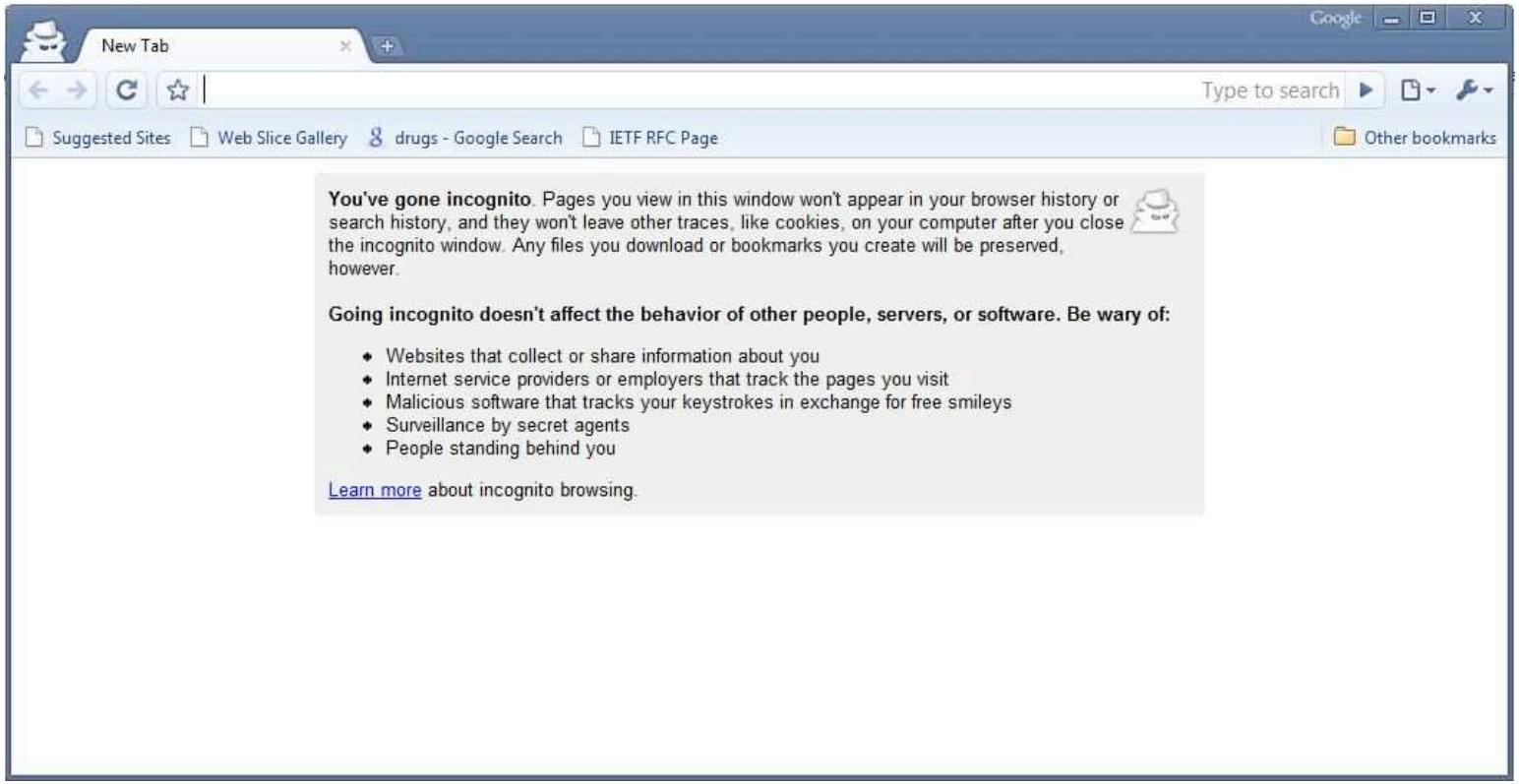
[11] PithHelmet supports a rule editor that allows users to set rules manually about objects to be blocked or allowed. These rules are expressed inje a language that the rule editor can interpret.

| Object Controls Comparison | Chrome | Internet Explorer 8 | Firefox 3.5 | AdBlock Plus Firefox Add-On | Safari | PithHelmet Safari Add-On | Opera 10 |
|---|---|---|---|---|---|---|---|
| **Users can manually allow objects (other than cookies).** | No | Yes | Yes | Yes | No | Yes | Yes |
| **Restrictions on which objects can be allowed:** | | Third party objects that appear on automatically generated list | Images only | Objects expressible in AdBlock filter language | | Objects expressible in PithHelmet rule editor | Images, Java, Javascript, CSS |
| **Supports allow lists.** | No | Yes, with InPrivate Filtering. | No | Yes | No | No | Yes |
| **Supports automatic updating of allow lists.** | No | No | No | Yes | No | No | No |
| **Controls can operate on a per-window basis.** | No | Yes | No | No | No | No | No |
| **Controls persist even when user quits and restarts browser.** | No | No | No | Yes | No | Yes | Yes |

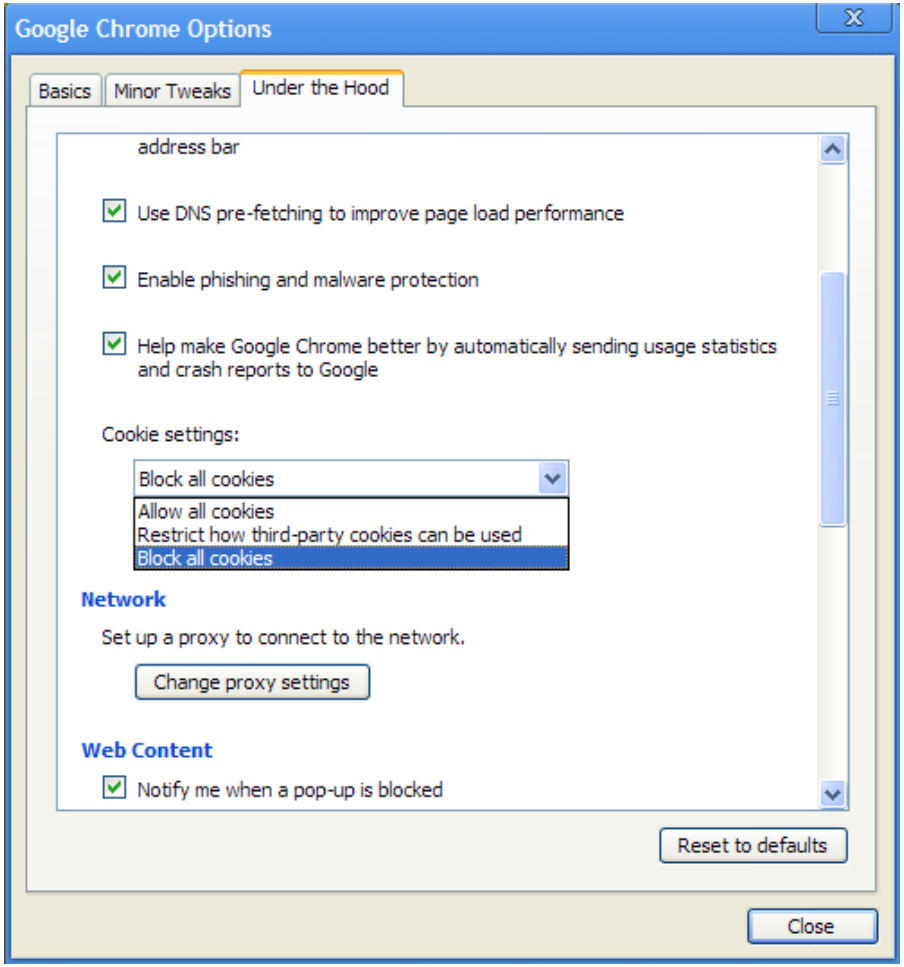
# Appendix: Browser Privacy Screenshots

## August 2009 – Version 2.0

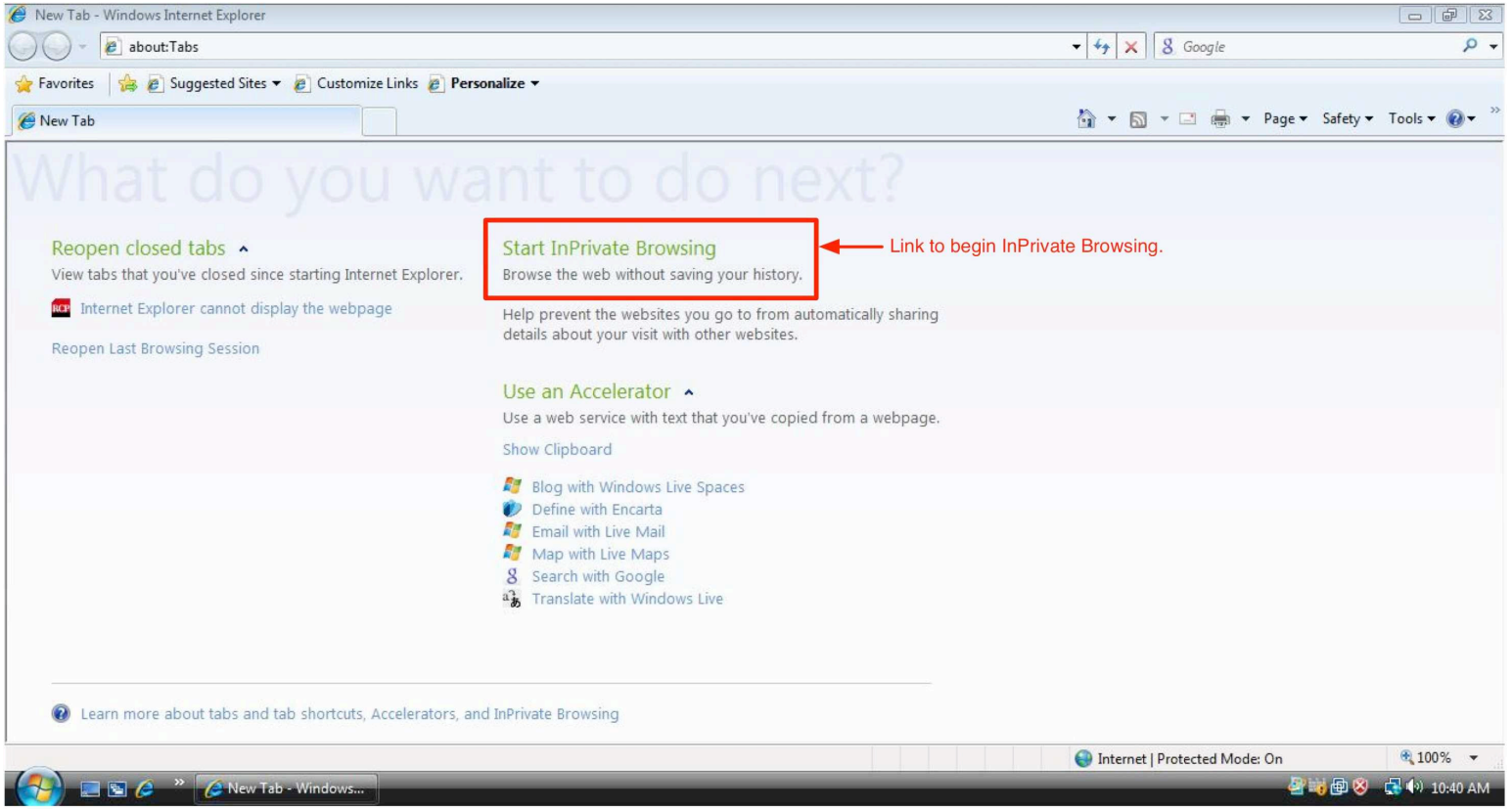
**Google Chrome Privacy Mode:**



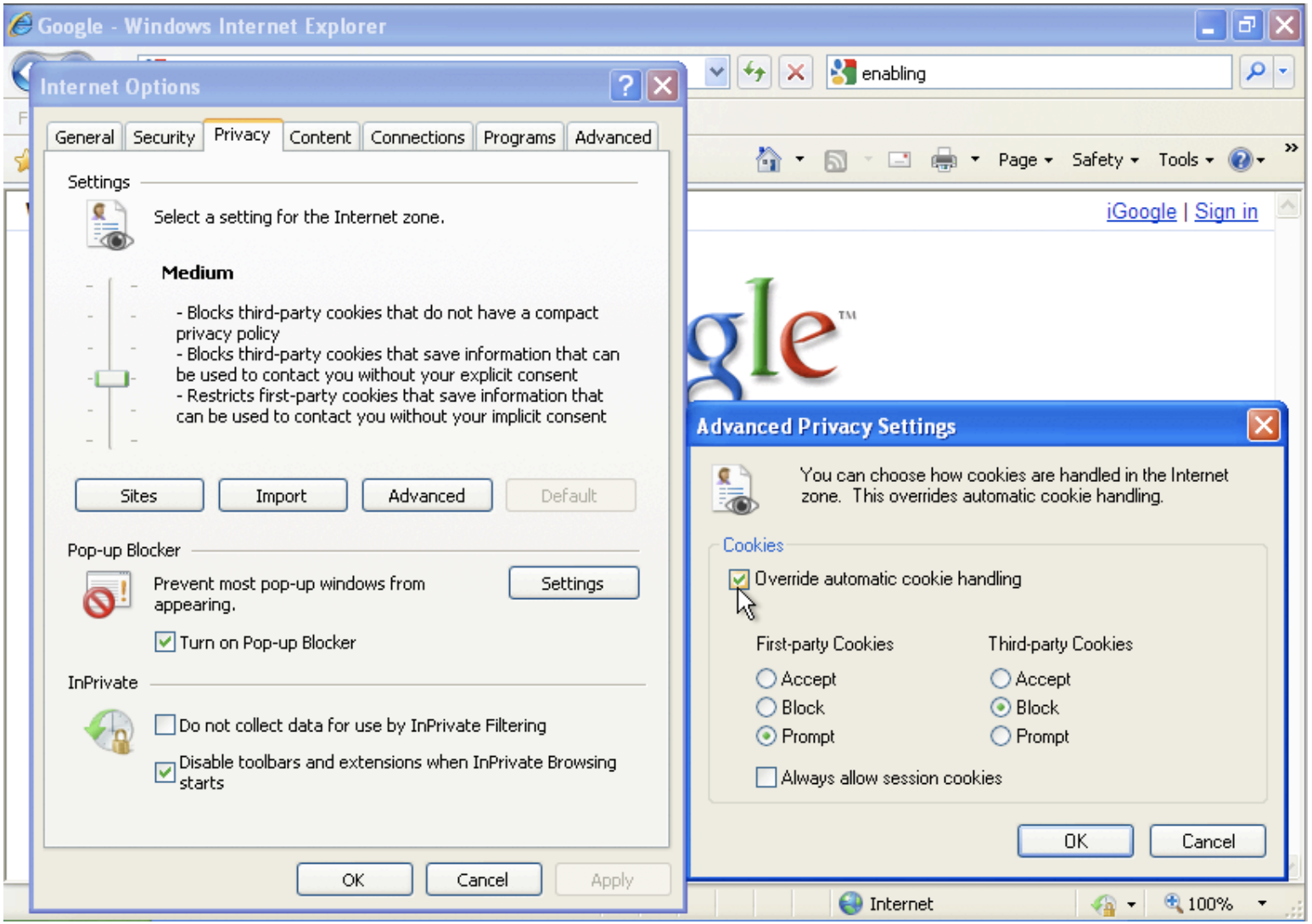
**Google Chrome Cookie Controls:**



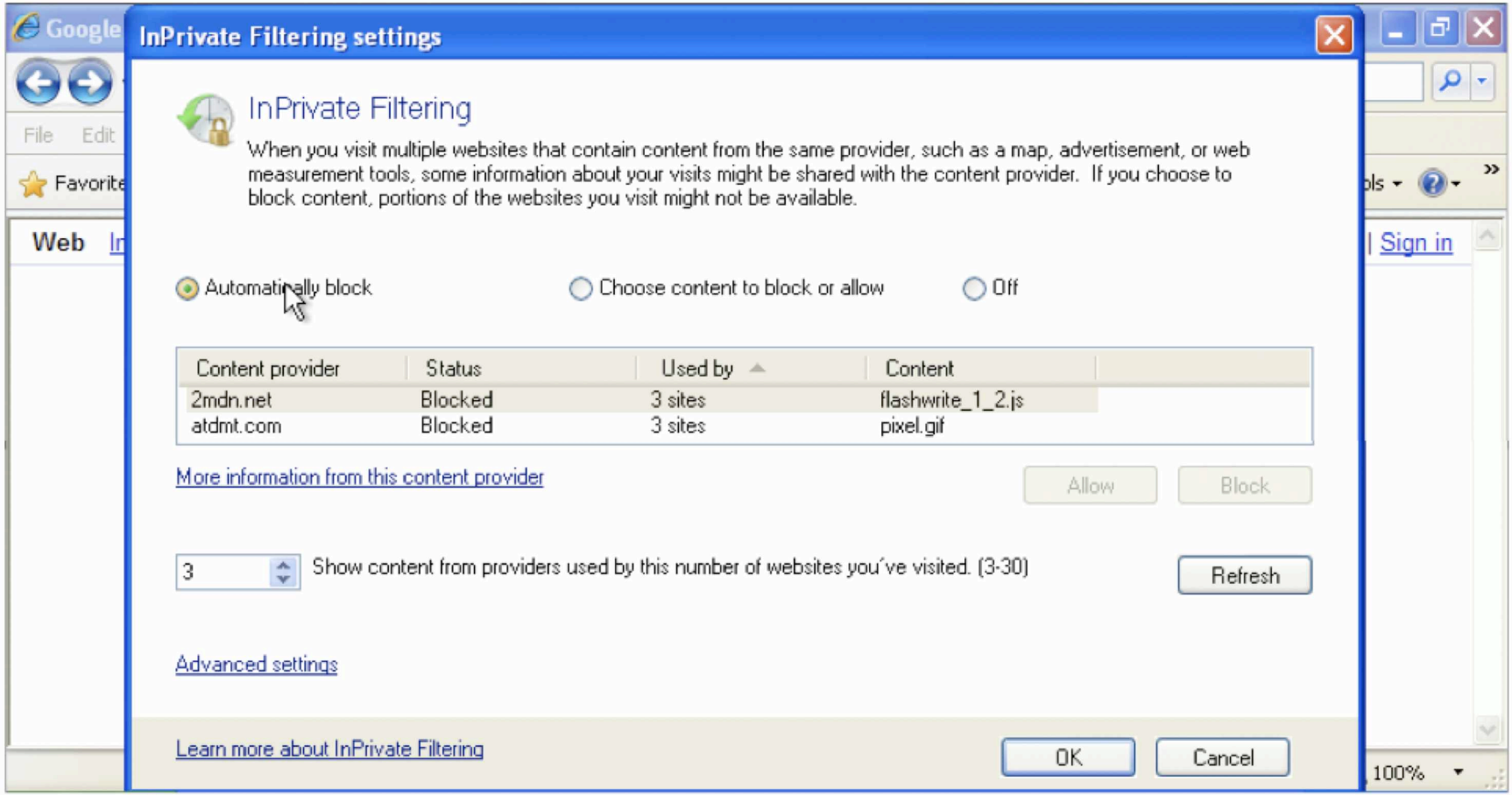
**Internet Explorer 8 Privacy Mode:**



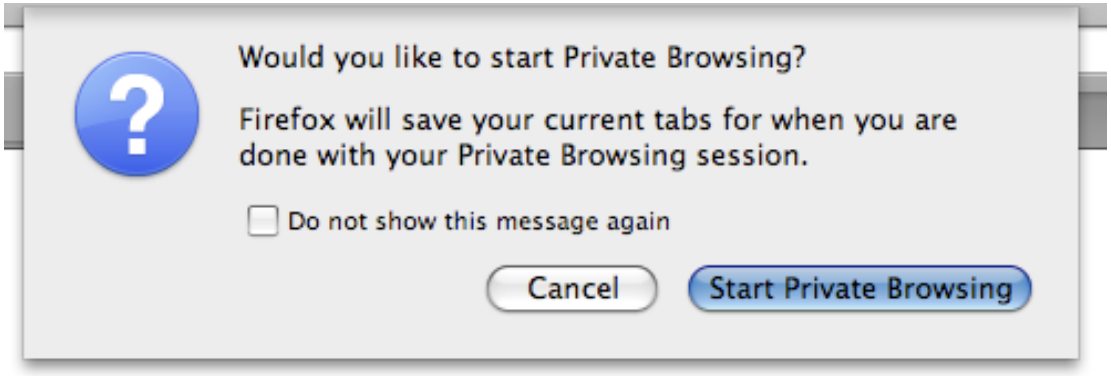
**Internet Explorer 8 Cookie Controls:**



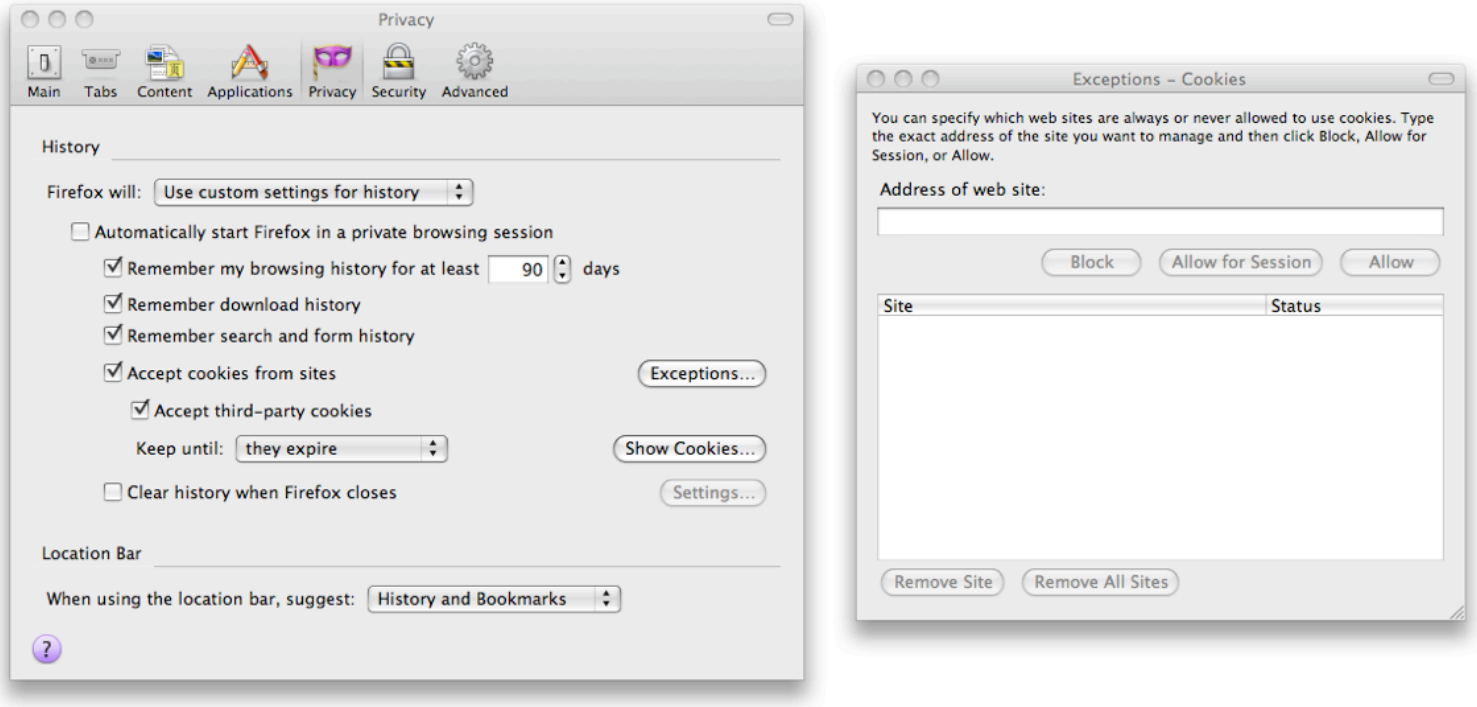
**Internet Explorer 8 Object Controls:**



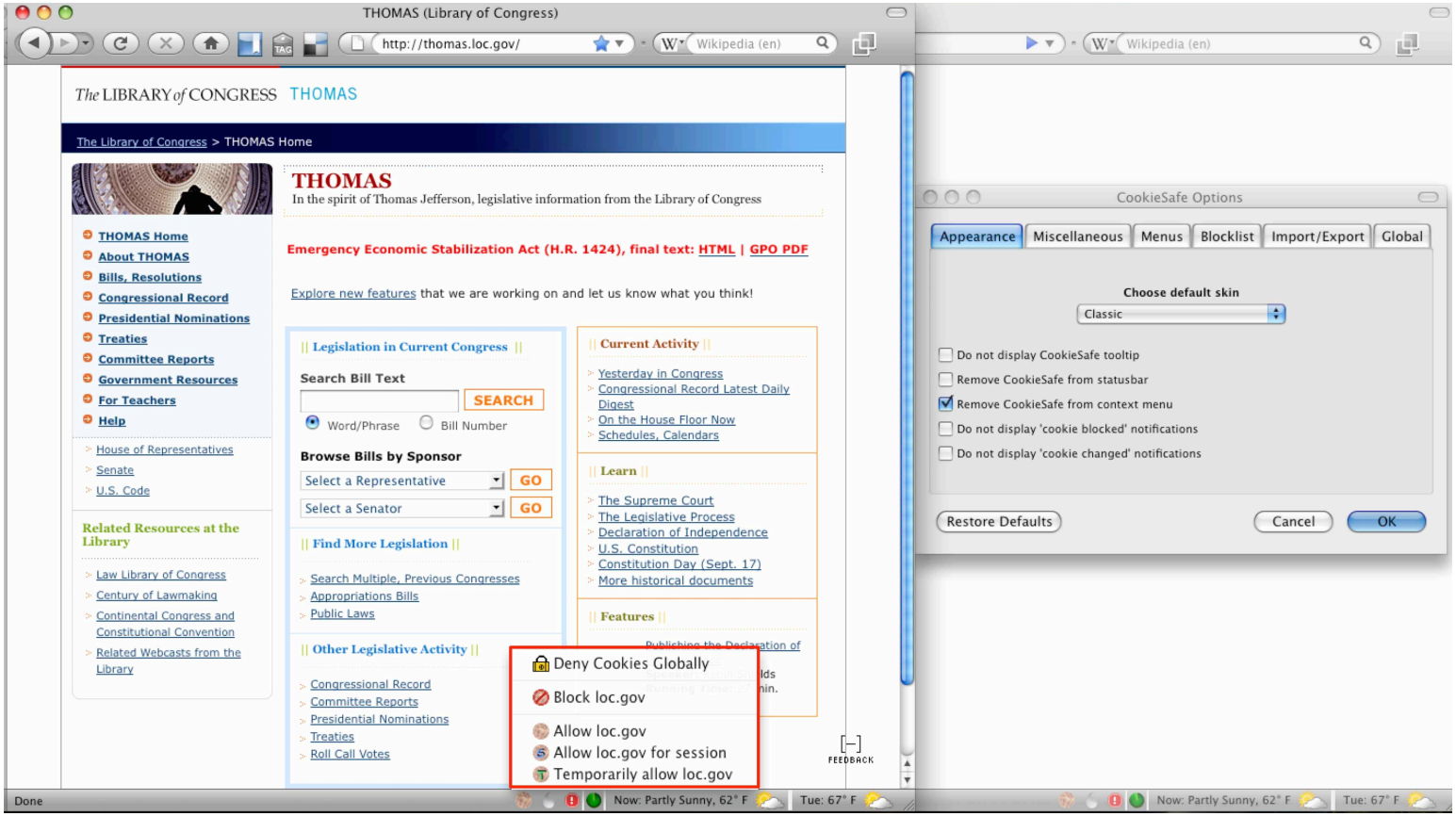
**Mozilla Firefox Private Browsing:**



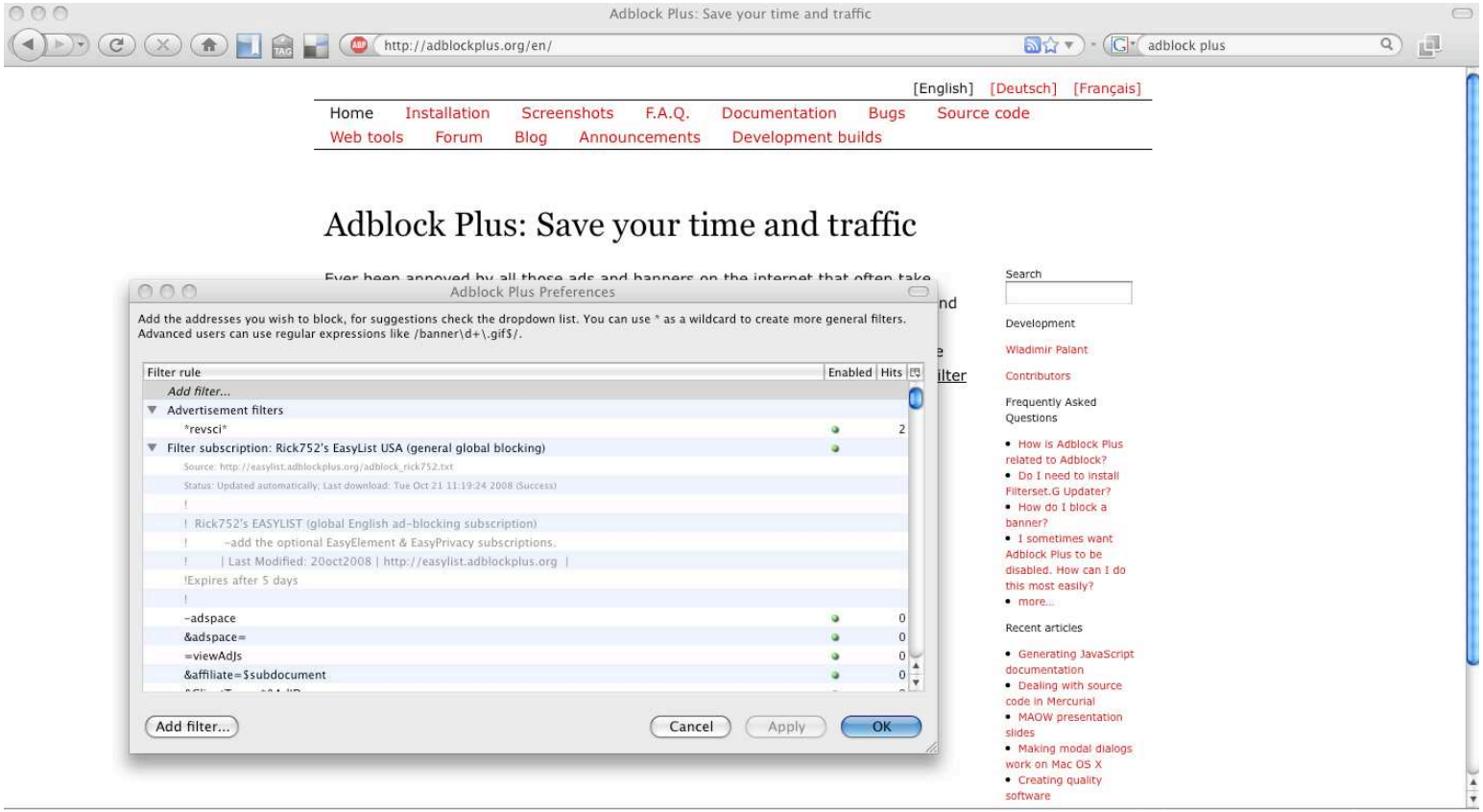
**Mozilla Firefox Cookie Controls:**



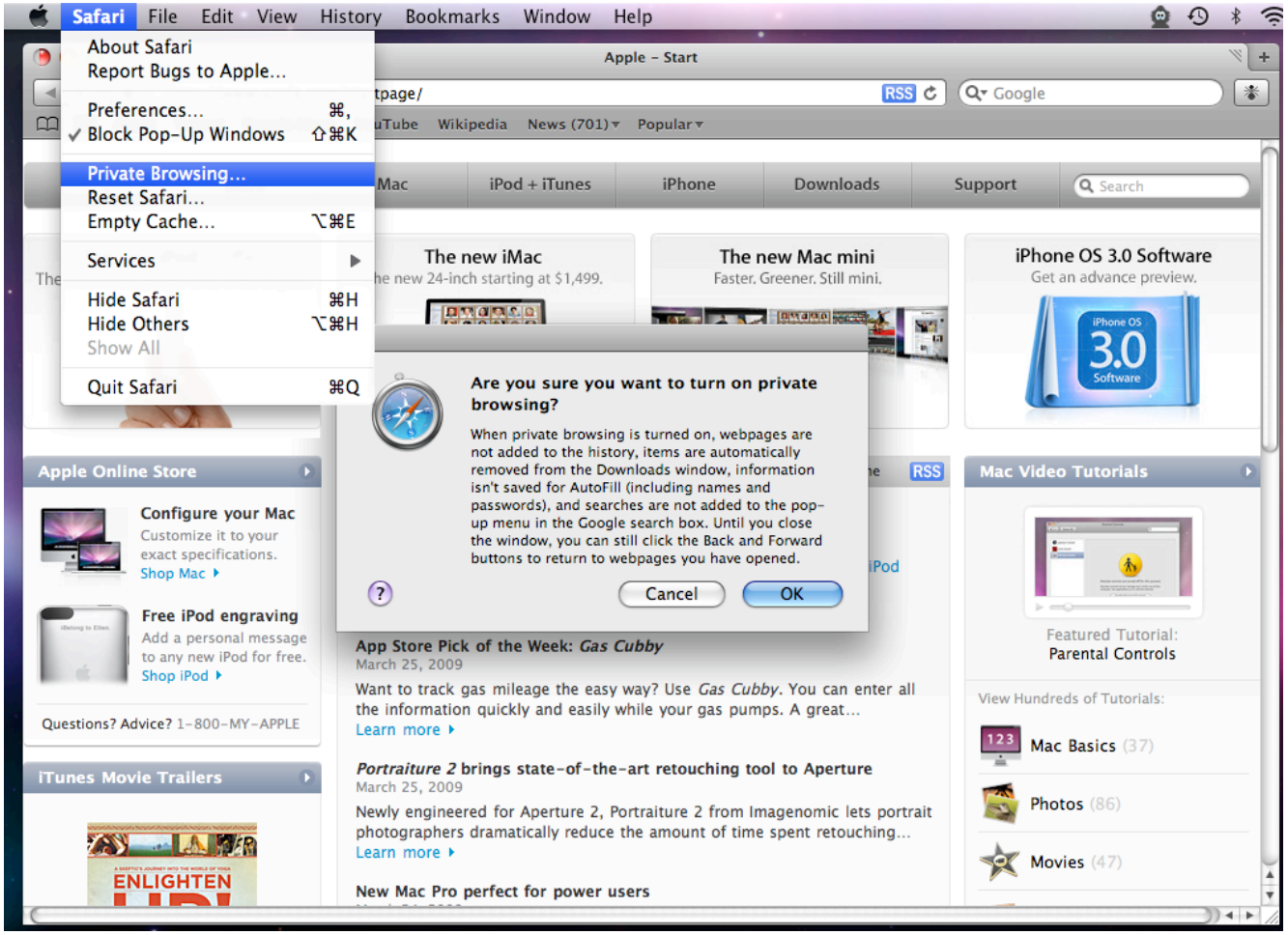
## Mozilla Firefox CookieSafe Add-On Cookie Controls:



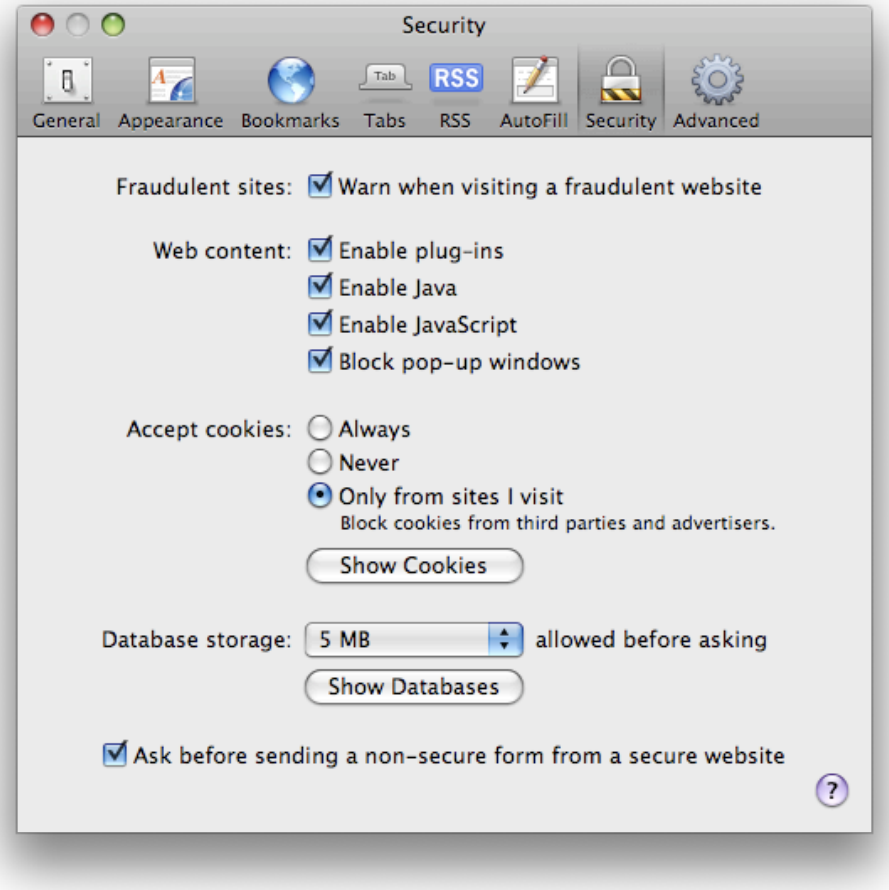
**Mozilla Firefox AdBlock Plus Add-On Object Controls:**



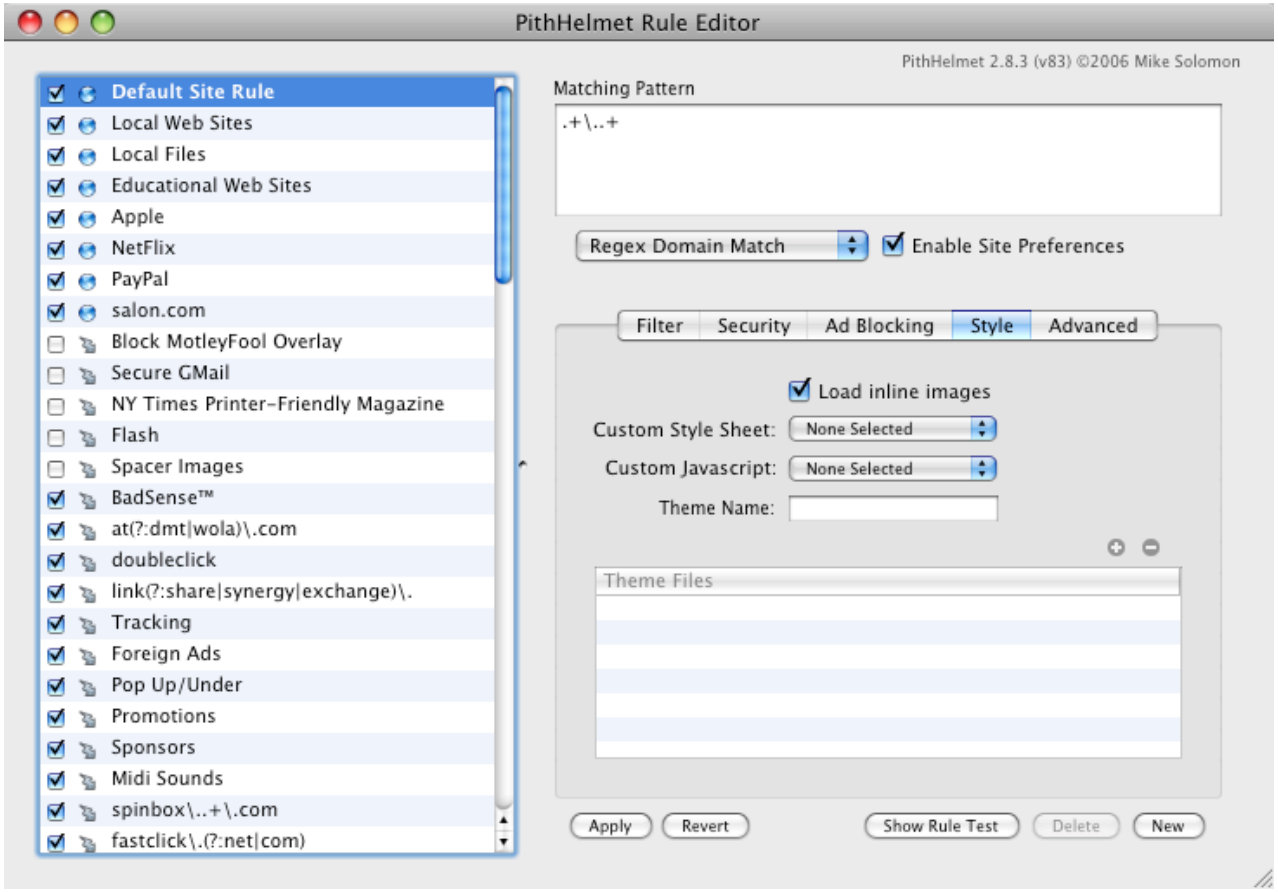
**Safari 4 Privacy Mode:**



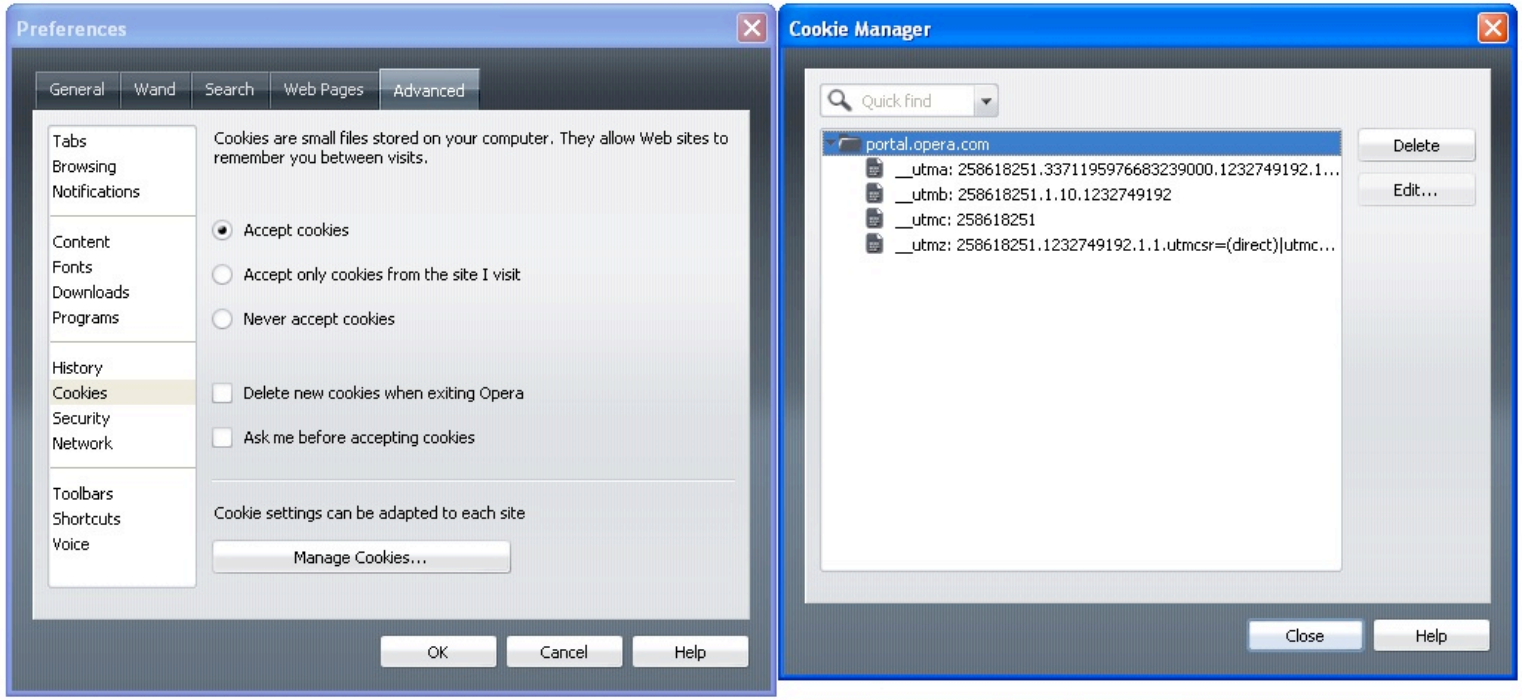
**Safari 4 Cookie Controls:**



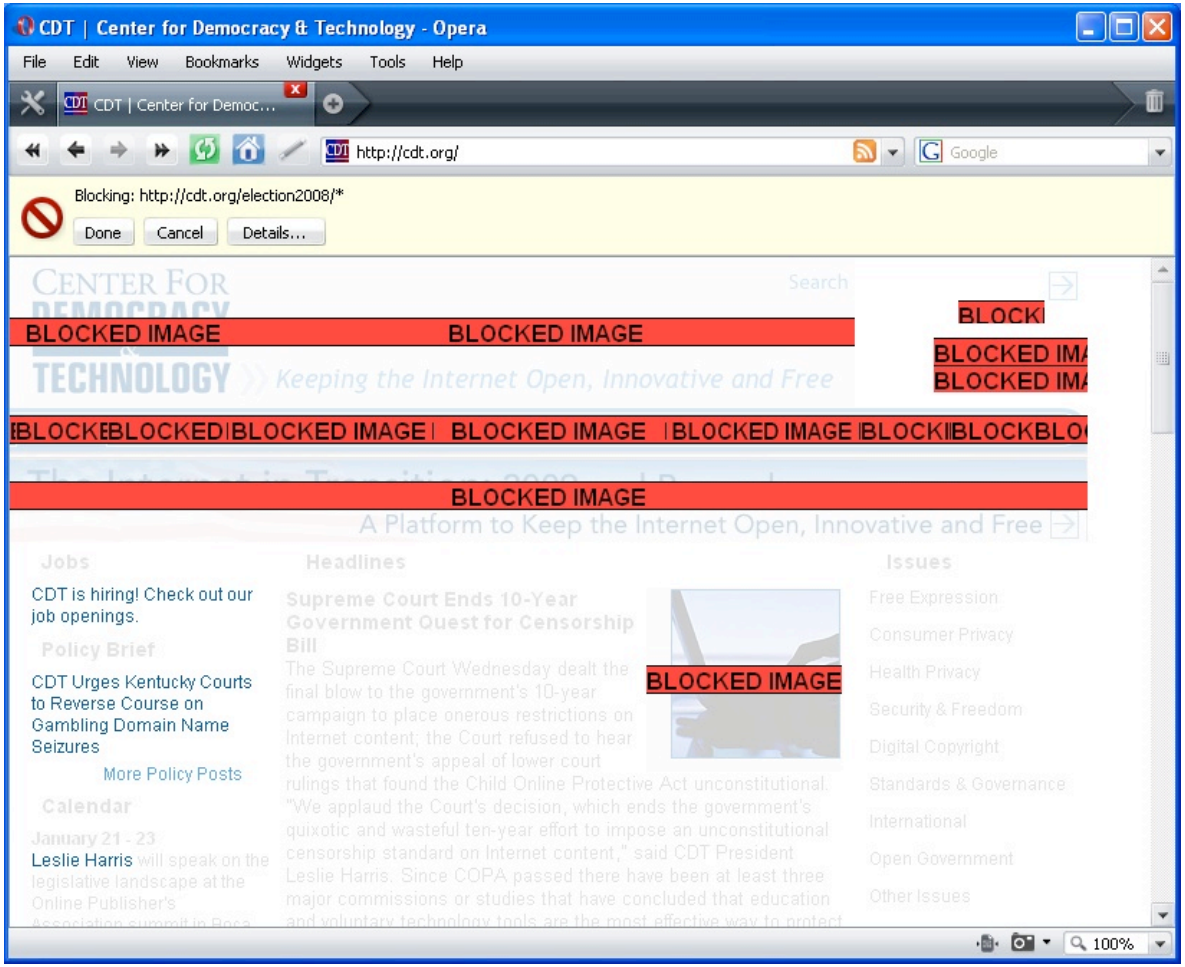
**Safari PithHelmet Add-On Object Controls:**



**Opera Cookie Controls:**



**Opera Object Controls:**



**FOR MORE INFORMATION**

Please contact: Brock Meeks
Director of Communications
202-637-9800