Browser Privacy Features: A Work In Progress

CDT Report -- 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 report compares the privacy features available in four Web browsers – Firefox 3, Internet Explorer 8 Beta 2, Google Chrome, and Safari 3. 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: Stealther for a Firefox privacy mode, CookieSafe for cookie controls in Firefox, AdBlock Plus for object controls in Firefox and PithHelmet for object controls in Safari.

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 and Mozilla 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.

For further information, contact:
Alissa Cooper (202) 637-9800 x110.

Privacy Mode Comparison

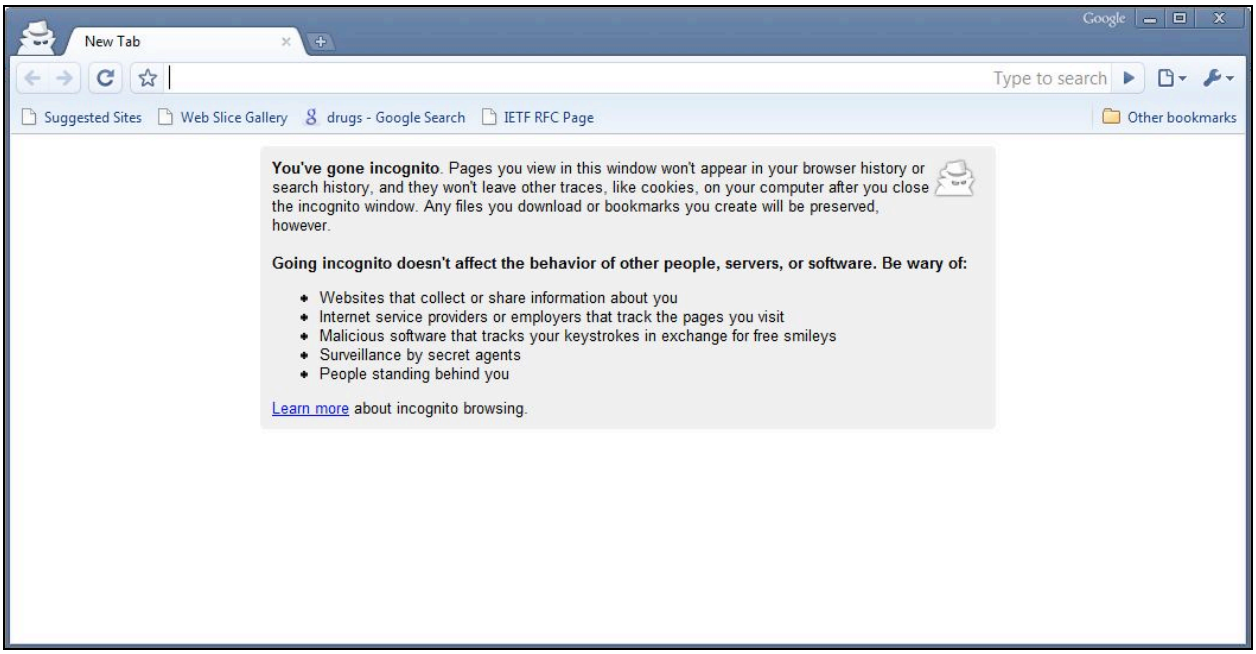
Each of the browsers provides some sort of privacy browsing mode. This mode is generally aimed at reducing or eliminating the storage of data locally on the user's computer. In some cases, this mode also affects data – specifically, cookies – transmitted by the browser.

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

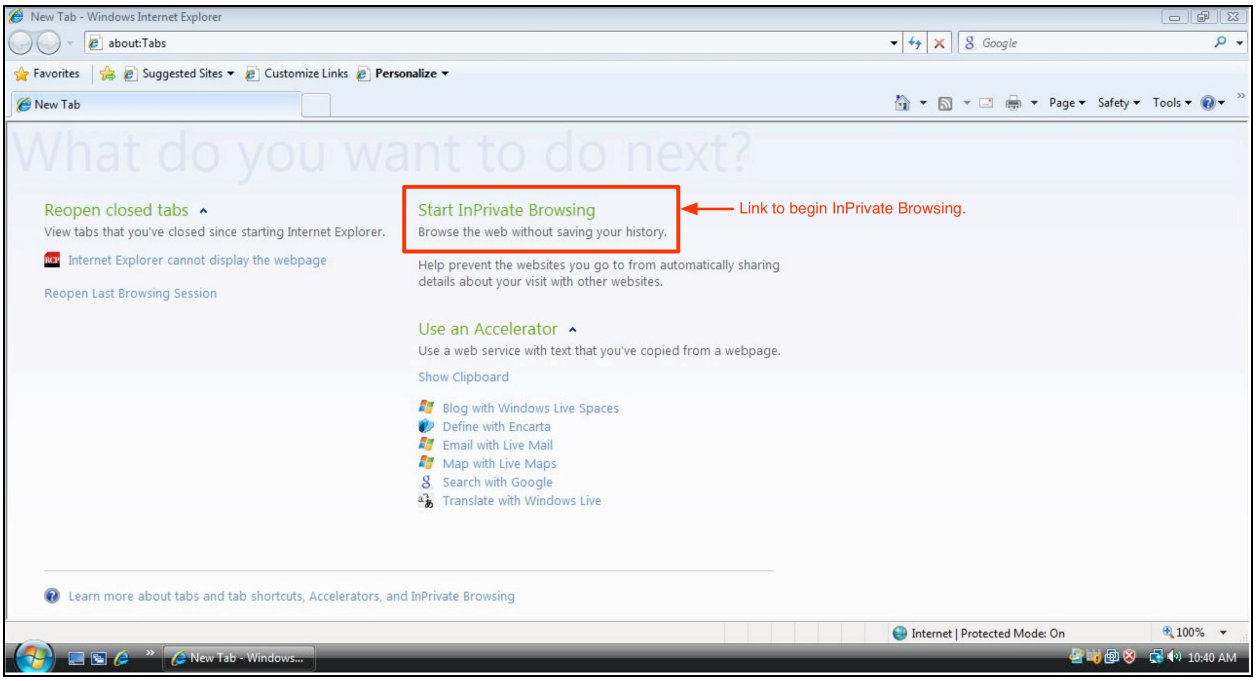
[i] With IE8's InPrivate Blocking (which is turned on by default during InPrivate Browsing), all objects served or requested by third parties from unique domains more than 10 times are blocked, which blocks cookies from being set or read from those domains.

[ii] 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.

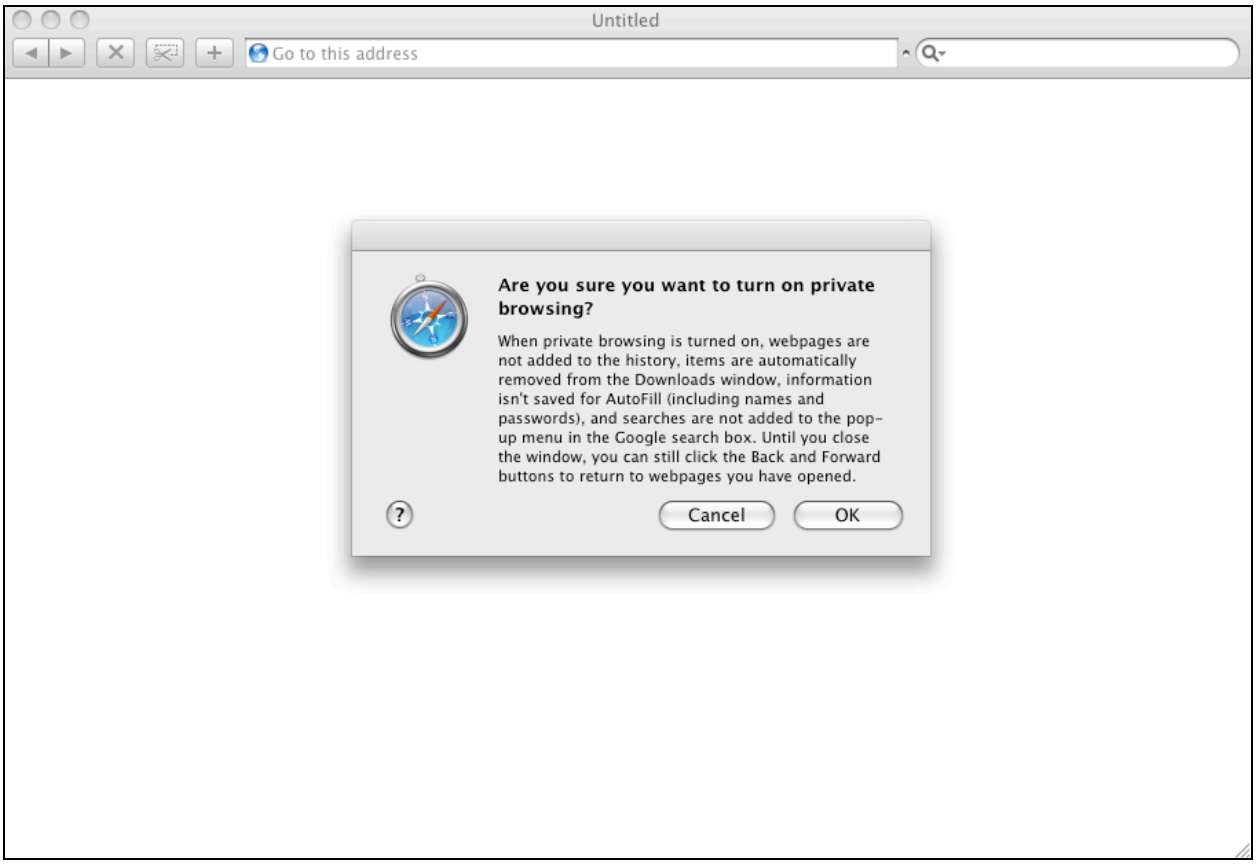
Chrome's Incognito:



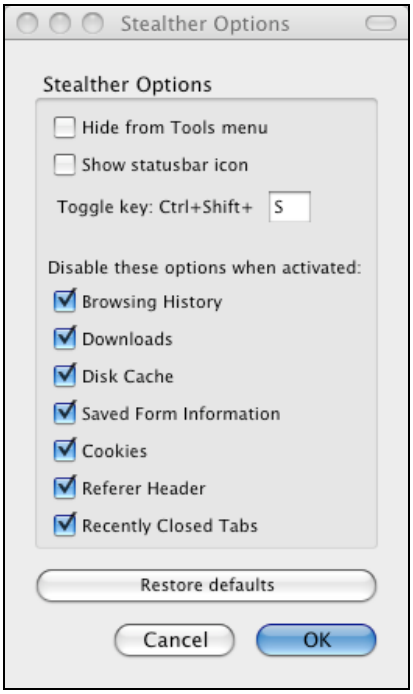
IE 8 Beta 2's InPrivate Browsing:



Safari's Private Browsing:



Stealther Firefox add-on:



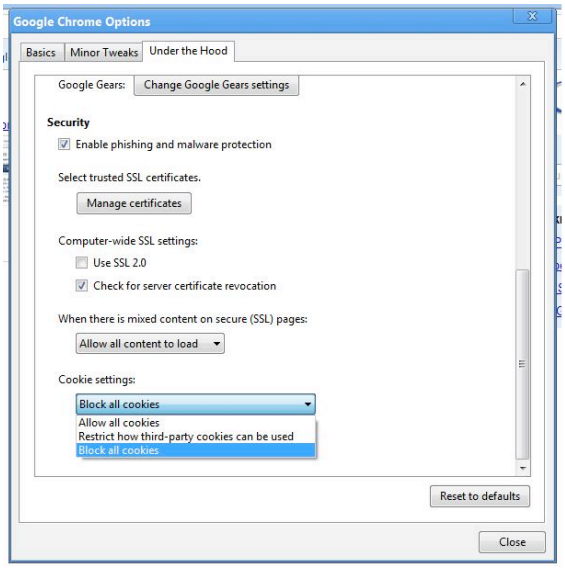
Cookie Controls Comparison

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.

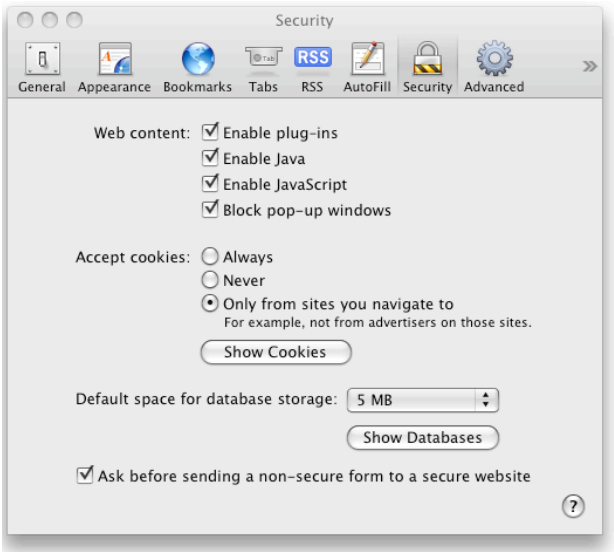
Cookie Controls Comparison	Chrome	Internet Explorer 8 Beta 2	Firefox	CookieSafe Firefox Add-On	Safari
Global first-party cookie options.	• Block • Allow	• Block • Allow • Prompt • Allow session cookies • Block or restrict according to automated privacy policy[i]	• Block (allow setting but not reading) • Allow • Prompt	• Block • Allow	• Block • Allow
First-party cookie default setting.	Allowed	Allowed, with cookies restricted according to automated privacy policy	Allowed	Allowed	Allowed
Global third-party cookie options.	• Block • Allow • Restrict: Allow setting but not reading	• Block • Allow • Prompt • Allow session cookies • Block or restrict according to automated privacy policy	• Block • Allow	• Block • Allow	• Block • Allow
Third-party cookie default setting.	Allowed	Allowed, with cookies blocked according to automated privacy policy	Allowed	Allowed	Blocked
Granular (per-site) cookie options.	None	• Block • Allow • Privacy import option for more specificity[ii]	• Block • Allow • Allow only on a session basis	• Block • Allow • Allow for current session • Allow only on a session basis[iii]	None
Cookie retention options.	None	Privacy import option allows specificity	• Until manually deleted • Until browser is closed • Prompt each time	• Until manually deleted • Until browser is closed • Prompt each time • User-specified retention time	None
Blocking cookies from being set prevents existing cookies from being read.	Yes	When blocking is set via privacy setting, yes. When blocking is set via advanced controls, no.	Yes	Yes	No
Can automatically prevent deleted cookies from being reset.	No	No	No	Yes	No

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

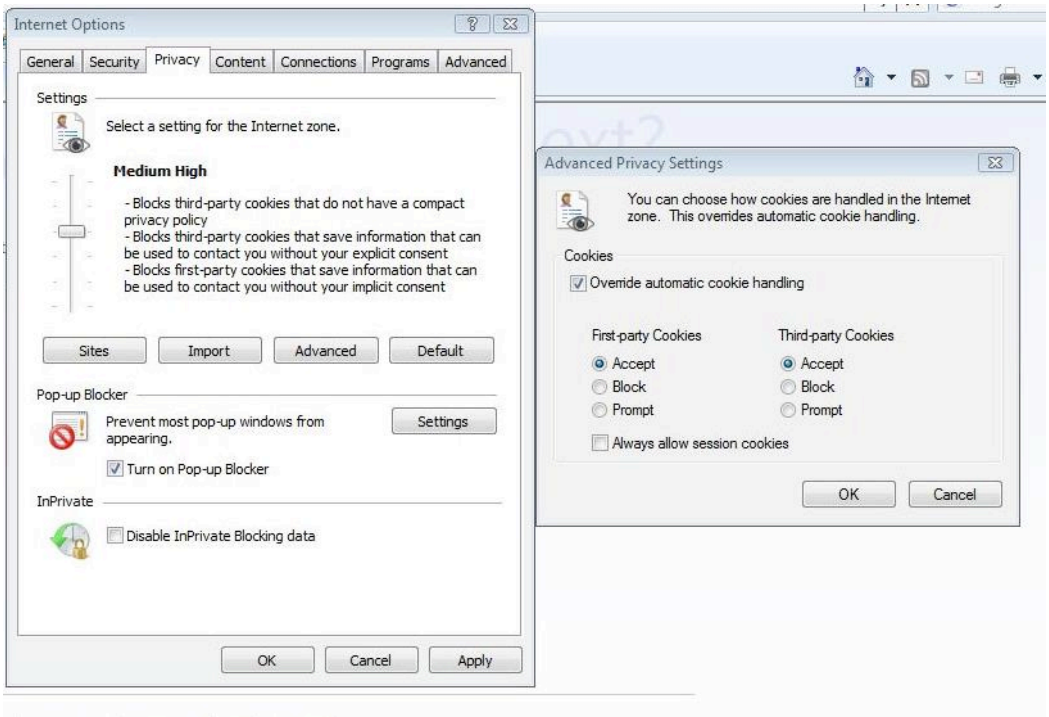
Chrome cookie controls:



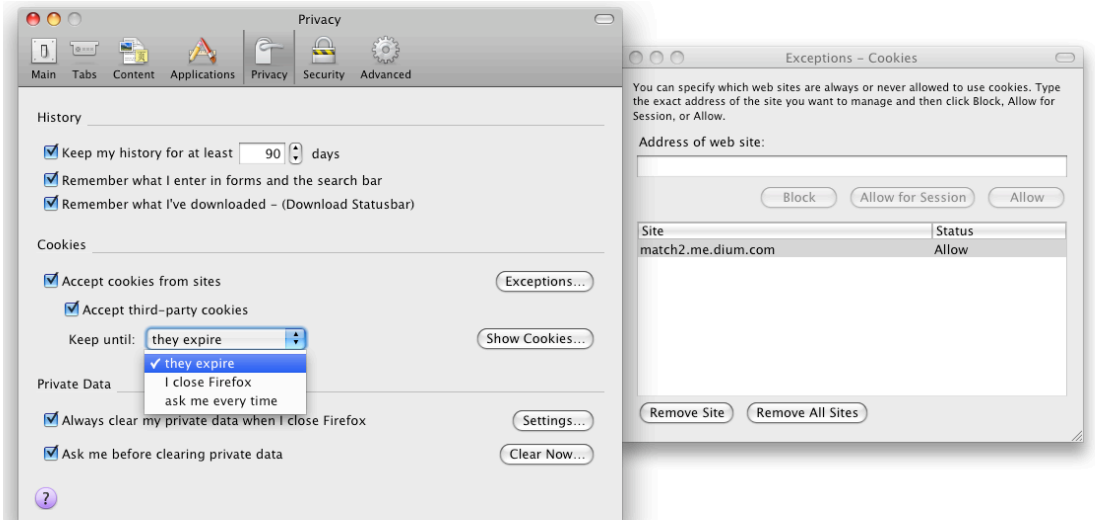
Safari cookie controls:



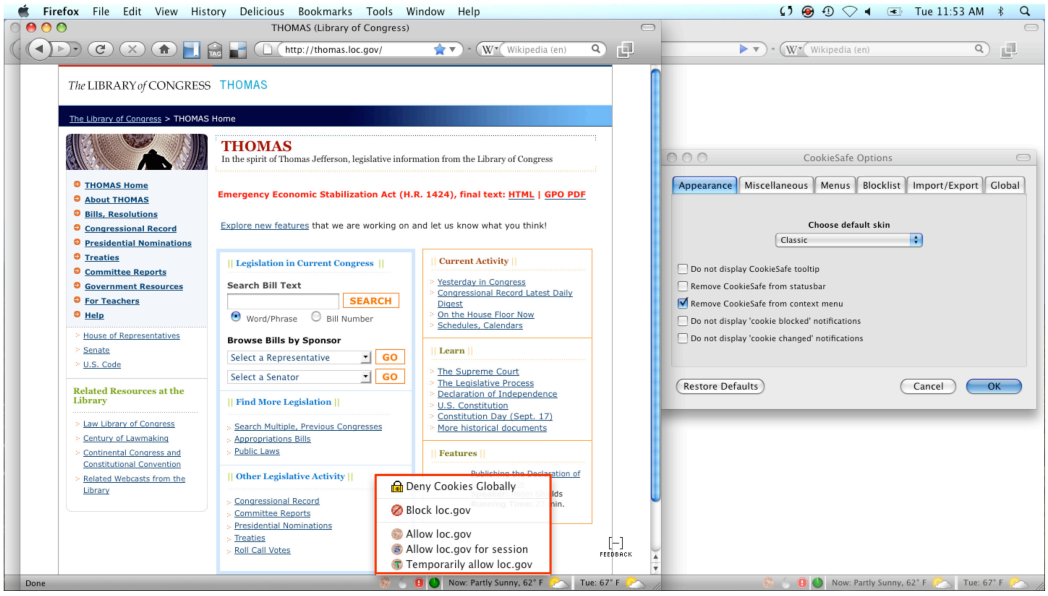
IE 8 Beta 2 cookie controls:



Firefox cookie controls:



CookieSafe Firefox add-on:



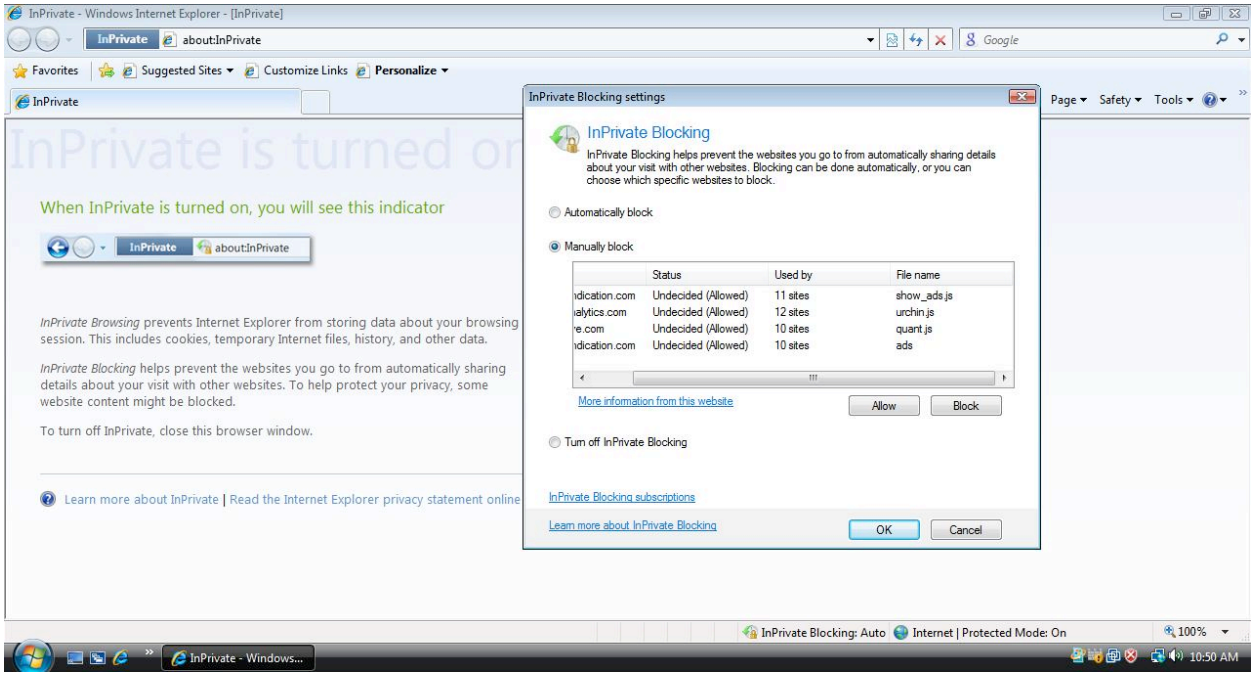
Object Controls Comparison

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.

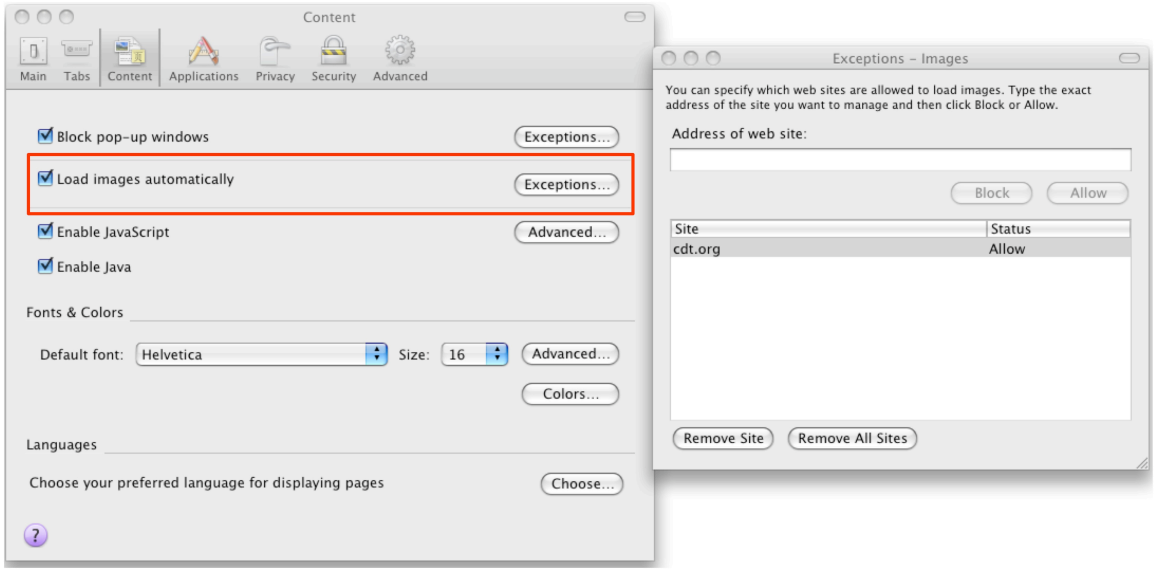
Object Controls Comparison	Chrome	Internet Explorer 8 Beta 2	Firefox	AdBlock Plus Firefox Add-On	Safari	PithHelmet Safari Add-On
Automatically blocks some objects. **Objects blocked:**	No	Yes, with InPrivate Blocking. All objects served or requested from unique domains by third parties more than 10 times.[i]	No	No	No	Yes Blocks a selection of ad servers and other domains by default.
Users can manually block objects (other than cookies). **Restrictions on which objects can be blocked:**	No	Yes, with InPrivate Blocking. Objects must appear on automatically generated list	Yes Images only	Yes Object must be expressible in AdBlock filter language[ii]	No	Yes Object must be expressible in PithHelmet rule editor[iii]
Supports block lists.	No	Yes, with InPrivate Blocking.	No	Yes	No	No
Supports automatic updating of block lists.	No	Yes, with InPrivate Blocking.	No	Yes	No	No
Users can manually allow objects (other than cookies). **Restrictions on which objects can be allowed:**	No	Yes, with InPrivate Blocking. Objects must appear on automatically generated list	Yes Images only	Yes Object must be expressible in AdBlock filter language	No	Yes Object must be expressible in PithHelmet rule editor
Supports allow lists.	No	Yes, with InPrivate Blocking.	No	Yes	No	No
Supports automatic updating of allow lists.	No	Yes, with InPrivate Blocking.	No	Yes	No	No
Controls can operate on a per-window basis.	No	Yes	No	No	No	No
Controls persist even when user quits and restarts browser.	No	No	No	Yes	No	Yes

[i] Subdomains are not considered as separate unique domains and do not increase this count.
[ii] 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.
[iii] PithHelmet supports a rule editor that allows users to set rules manually about objects to be blocked or allowed. These rules are expressed in a language that the rule editor can interpret.

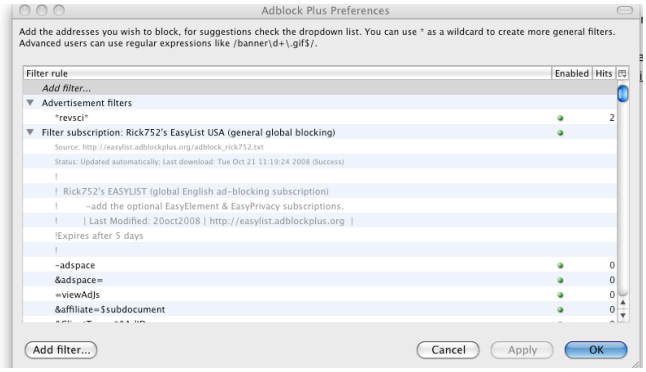
IE 8 Beta 2 object controls:



Firefox object controls:



AdBlock Plus Firefox add-on:



PithHelmet Safari add-on: