KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

BROWSER PRIVACY FEATURES: A WORK IN PROGRESS

December 2010 – Version 3.0

This report reviews the privacy features available for the latest versions of Mozilla Firefox, Microsoft Internet Explorer, Google Chrome, Apple's Safari, and Opera's Web browser. We find that features have improved so that consumers can reduce the amount of personal information they transmit online or leave behind on their computers, but at the same time both the complexity of the controls and the diversity of online tracking methods leave consumers little better off. This is an update to version 2.0 of this report, which was released in August 2009.

The browser is the gateway to the Internet for most consumers. Providing browser privacy controls that are robust, easy to find, and simple to use is crucial to empowering consumers to maintain their privacy online. Improvements in browser controls cannot replace the need for a comprehensive national privacy law, but they can go a long way towards helping consumers exercise some control of their own data.

In the last six months, all of the major browser makers have released versions of their products with new privacy features. That these companies are competing to provide better privacy protections is great news for Internet users. The browser makers are in an excellent position to further develop their existing controls and provide new features aimed at giving Internet users greater control over their privacy as they surf the Web. CDT will continue to revisit the browser space to assess whether companies continue to improve the strength, simplicity and accessibility of browser privacy controls.

In this report, we examine the privacy features[1] available in five Web browsers – Chrome 7, Firefox 3.6 and 4.0 beta 6, Internet Explorer 8 and 9 Beta, Opera 10.6, and Safari 5.[2] In the charts below, we compare the features offered by each browser in five areas: general privacy controls, privacy modes, cookie controls, object controls, and geolocation controls. All of the browsers were tested on Windows 7, except for Safari, which was tested on Mac OS X, where it is predominantly used. We provided a draft of this document to Apple, Google, Microsoft, Mozilla, and Opera several

[1] Only settings that are available to an end-user through the browser's interface are addressed by this report. Although sophisticated controls, such as the ability to always start in privacy mode or to disable DOM storage, may be configurable by an advanced user through low level or command line configuration settings, if the controls are not directly exposed through the end-user interface, they are generally not addressed.

[2] Firefox 3.6 and 4.0 beta 6 are listed together, as are Internet Explorer 8 and 9 Beta, because there was no difference between the beta version and the current release in terms of the privacy controls that they provided at the time of writing.

weeks in advance to allow them to verify the accuracy of the claims made in the report about their browser software. Where appropriate, we have revised the report in response to the feedback we received from those companies.

Summary: No one browser stands out as the clear privacy leader. All have relative strengths and all have relative weaknesses; depending on how you use the Web (e.g. for location-enabled services or for "private browsing" mode), a different browser may be the most privacy protective for you. In general, all five browsers now offer more user controls for privacy than they did when CDT last issued this report in August of 2009. At the same time, however, browsers also present more ways for consumers to transmit personal information, for example by offering precise location-based services and local storage that allow consumers to be tracked in new ways. The fact that this report has expanded from 10 pages in its last version to its current 19 pages is a blessing and a curse for consumers: there are more controls but more exposure as well, and it is becoming increasingly difficult for consumers to shut down all potential avenues for unwanted sharing on the Internet.

One potential solution to the complexity of user choices would be the implementation through the browser of a "Do Not Track" mechanism that would allow consumers to set persistent and global tracking preferences. If done correctly, the incorporation of a "Do Not Track" feature in the browsers could represent an improvement for consumers who wish to exercise more control over their information sharing online. CDT first proposed the idea of "Do Not Track" in 2007 along with a group of other public interest organizations. The information ecosystem has become radically more complicated since that time, and the concept of "Do Not Track" has attracted new attention recently. The online advertising industry has been discussing ways to create such controls through self-regulation, and Congress is considering whether "Do Not Track" should be included as a part of a general baseline privacy law. Both Microsoft and Mozilla have announced promising efforts in recent days to eventually offer these sorts of global opt-out options to consumers. However implemented, "Do Not Track" is not a replacement for baseline privacy legislation, which is needed to address the full range of privacy issues, not just Web-based behavioral advertising.

One further thing to note: the report only looks at what information browsers store about a user or allow to be transmitted to third parties. It does not address the issue of browser security, nor does it address what information the browser maker itself may receive about a user's web activity.

The browser report is divided into five general sections:

General Privacy Controls: When an Internet user visits a webpage, her browser sends information to the entities involved in delivering the content that constitutes the webpage. The entities to which information is disclosed include the website that the user navigates to, but may also include third parties that provide content, Web beacons, or other components to the webpage. At the same time, in the normal course of Web surfing, browsers record and retain information about browsing activity locally on users' computers. This includes a history of visited websites, downloaded files, and search terms. Browsers can also save the data typed into online forms (including passwords) and cached versions of files. General privacy controls allow the user to proactively clear information that the browser has collected during the course of Web browsing. The controls may also prevent the browser from sending certain information, such as the referring URL, to websites. All of the browsers provide controls to automatically clear some stored information, although the information that can be cleared is different for each browser.

Privacy Mode: The main motivations behind a browser privacy mode are to allow users to browse without leaving data trails on their computers and to limit the information given to remote parties. The privacy modes in each of the browsers reduce the local storage of these kinds of information, thereby providing increased privacy on shared computers. All of the browsers now provide a privacy mode, although their functionality varies slightly.

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.

Object Controls: Cookies are not the only tracking mechanism available to websites and services. Browsers receive and transmit content of many different types – everything from basic text and images to style sheets, scripts, local shared objects (sometimes called "flash cookies"), and more. These kinds of data may also be used to log and profile the user's Web activities when repeatedly transmitted to or from a user's browser across different sites. In this report we use the term "object controls" to describe all other browser mechanisms that allow users to decide what content to block or allow on their computers.

Geolocation Controls: Websites are increasingly providing services that use information about the location of a computer. Geolocation controls indicate when geolocation information is being provided to a site and enable users to manage when their geolocation is provided. Geolocation controls are an area where browser controls markedly differ.

Summary of Key Differences

Key Differences	Chrome 7	Firefox 3.6 / 4.0 beta 6	Internet Explorer 8 / 9 Beta	Opera 10.6	Safari 5
Can be persistently configured to clear all browsing data	Limited	Yes	Yes	Limited	Limited
Can delete the browsing history for a specific site	No	Sub-domain level	No	No	No
Referring URL can be disabled	No	No	No	Yes	No

Key Differences	Chrome 7	Firefox 3.6 / 4.0 beta 6	Internet Explorer 8 / 9 Beta	Opera 10.6	Safari 5
Privacy mode can be set to automatically start when browser is launched	No	Yes	No	No	No
Third-party cookie default setting	Allowed	Allowed	Allowed	Allowed	Disabled
Blocking third-party cookies / accepting cookies only from site visited prevents acceptance of third-party cookies	Yes	Yes	Yes	No	Yes
Blocking third-party cookies / accepting cookies only from the site visited prevents first-party cookies from being used later as a third-party cookie	No	Yes	No	No	No
Controls for DOM storage settings	• Allow • Disable • Prompt • Session only	No	• Allow • Disable	• Allow • Disable • Prompt	No
Controls for other local storage	No	No	No	No	No
Provides a geolocation indicator	Yes	No	NA[3]	Yes	No
Centralized management of geolocation permissions	Yes	No	NA	No	No

[3] Geolocation privacy controls are not applicable to Internet Explorer 8 and 9 Beta because they do not support geolocation services.

General Privacy Controls Comparison

All of the browsers provide a control that allows the user to clear some or all of the data that is collected by the browser and stored locally. Many of these settings can be persisted so that specific types of information are automatically cleared at the end of each browsing session. Some browsers also provide options that allow users to restrict information, such as the referring URL, that is sent to remote parties.

General Privacy Controls	Chrome 7	Firefox 3.6 / 4.0 beta 6	Internet Explorer 8 / 9 Beta	Opera 10.6	Safari 5
Types of data clearable by the "clear private data now" option	• Temporary files (cache)	• Temporary files (cache)	• Temporary files (cache)	• Temporary files (cache)	• Temporary files (cache)
	• All cookies (including DOM storage)	• All cookies	• All cookies	• All cookies • Temporary cookies	• All cookies
	• Browsing history	• Browsing history	• Browsing history	• Browsing history	• Browsing history
	• Download history	• Download history	• Download history	• Download history	• Download history
	• Form data	• Form data	• Form data	• NA[4]	• Form data
	• Saved passwords	• Saved passwords[5]	• Saved passwords	• Saved passwords	
		• Search history • Active logins • Site preferences	• InPrivate Filtering data	• Persistent storage • Bookmark visited time • Email account passwords	• Top sites • Webpage preview images • Website icons • Location warnings

[4] The ability to clear form data is not applicable to Opera because Opera does not automatically store form data.

[5] The "clear recent history" feature does not actually include the option to clear saved passwords, however the control is listed here because saved passwords can be managed by going to Options-> Security-> Passwords.

General Privacy Controls	Chrome 7	Firefox 3.6 / 4.0 beta 6	Internet Explorer 8 / 9 Beta	Opera 10.6	Safari 5
Time ranges for which private data can be cleared	• Everything • Last 4 weeks • Last week • Last day • Last hour	• Everything • Last day • Last 4 hours • Last 2 hours • Last hour	• Everything	• Everything	• Everything
Granular control to delete a specific site	No	Sub-domain level[6]	No	No	No
Persistent setting to delete browsing history when browser is closed or to not remember browsing history	No	Yes	Yes	Yes	No
Persistent setting to delete download history when browser is closed	No	Yes	Yes	No	Yes
Persistent setting to delete search history when browser is closed	No	Yes	Yes	No	No
Persistent setting to delete form data when browser is closed or to disable auto-fill	Yes	Yes	Yes	Yes[7]	Yes
Persistent setting to delete saved passwords when browser is closed or to disable password saving	Yes	Yes	Yes	Yes	Yes
Persistent setting to delete cookies when browser is closed	Yes[8]	Yes	Yes	Yes	Yes

[6] Each permutation of a website's sub-domain needs to be removed separately (e.g. cdt.org, privacy.cdt.org, and content.cdt.org).

[7] Opera does not provide auto-fill functionality for forms except for data specified by the user through the Preferences→Forms interface.

[8] Chrome includes DOM storage deletion as part of cookie deletion.

General Privacy Controls	Chrome 7	Firefox 3.6 / 4.0 beta 6	Internet Explorer 8 / 9 Beta	Opera 10.6	Safari 5
Persistent setting to delete temporary cache when browser is closed	No	Yes	Yes	Yes	No
Does not store files opened by other applications in the browser history	Yes	Yes	No	Yes	Yes
Referring URL can be disabled[9]	No	No	No	Yes	No
Sources for address bar suggestions	• History • Bookmarks • Online search service[10]	• History • Bookmarks	• History • Bookmarks • Online search service[11]	• History • Bookmarks	• History • Bookmarks
Address bar suggestions can be disabled	Limited - can only disable online search service.	Yes	Yes	Limited - can only disable history.	No
Does not automatically send browsing history to an online service	Yes	Yes	Yes. The user must opt-in to the service.	Yes	Yes

[9] 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.

[10] Information typed in the address bar is automatically sent to an online search service to retrieve site suggestions based on the input.

[11] Internet Explorer 9 Beta has an integrated search service in the address bar. The user must opt-in to use this service.

Privacy Mode Comparison

All of the browsers today provide a privacy browsing mode. This mode is generally aimed at reducing or eliminating the storage of data locally on the user's computer and limiting the information given to remote parties. In some cases, this mode also affects data – specifically, cookies – transmitted by the browser. The privacy mode feature achieves results similar to the "clear private data" menu option.

Privacy Mode	Chrome 7: Incognito	Firefox 3.6 / 4.0 beta 6: Private Browsing	Internet Explorer 8 / 9 Beta: InPrivate Browsing	Opera 10.6: Private Tab / Window	Safari 5: Private Browsing
Does not keep visited sites in the browser history	Yes	Yes	Yes	Yes	Yes
Does not keep downloaded files in the download history[12]	Yes	Yes	Limited[13]	Yes	Yes
Does not save form fields data (including passwords)	Yes	Yes	Yes	Yes	Yes
Does not save addresses typed into the address bar	Yes	Yes	Yes	Yes	Yes
Does not remember visited links	Yes	Yes	Yes	Yes	Yes
Does not save search queries	Yes	Yes	Yes	Yes	Yes

[12] Although the browser may not directly store the download history, the files remain on the operating system until deleted.

[13] If a user opens the file, IE stores that information in the History under "Computer" and this history is not removed when the user leaves the InPrivate Browsing mode.

Privacy Mode	Chrome 7: Incognito	Firefox 3.6 / 4.0 beta 6: Private Browsing	Internet Explorer 8 / 9 Beta: InPrivate Browsing	Opera 10.6: Private Tab / Window	Safari 5: Private Browsing
Deletes cached files at the end of the browsing session	Yes	Yes	Yes	Yes	Yes
Does not read existing third-party cookies	Yes	Yes	Yes	Yes	Yes
Deletes new cookies at the end of the session	Yes	Yes	Yes	Yes	Yes
Blocks referring URL from being sent	No	No	No	No	No
Disables browser plug-ins[14]	No[15]	No	No	No	No
Disables browser extensions[16]	Yes	No	Yes	NA	No
Disables automatic online address bar search service (if browser supports)	Yes	NA	Yes[17]	NA	NA
Disables online site suggestion service (if browser supports)	NA	NA	Yes	NA	NA
Operates on a per-window basis	Yes	No	Yes	Yes	No

[14] A browser plug-in is a third party application that interacts with the browser, but does not run natively in the browser. An example of a plug-in is Adobe Flash Player.

[15] Chrome Incognito runs plug-ins in an off-the-record mode that sets a flag indicating user data should not be stored. However it is up to the plug-in to honor the flag.

[16] A browser extension (or add-on) runs natively in the browser. An example of an extension is AdBlock Plus for Firefox.

[17] Internet Explorer 9 Beta has an integrated search service in the address bar that users may choose to opt into when browsing in normal mode. In InPrivate Browsing this service is disabled by default. Users can re-enable it in the address bar during InPrivate Browsing if they choose to do so.

Privacy Mode	Chrome 7: Incognito	Firefox 3.6 / 4.0 beta 6: Private Browsing	Internet Explorer 8 / 9 Beta: InPrivate Browsing	Opera 10.6: Private Tab / Window	Safari 5: Private Browsing
Persists when user exits and re-starts the browser	No	No	No	No	No
Can be set to automatically start when browser is launched	No	Yes	No	No	No

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	Chrome 7	Firefox 3.6 / Firefox 4 beta 6	Internet Explorer 8 / 9 Beta	Opera 10.6	Safari 5
Global first-party cookie options	• Block • Allow	• Block • Allow • Prompt (allow, allow for session, deny)	• Block • Allow • Prompt • Allow, prompt, or reject as defined in a privacy settings file created by the user[18]	• Block • Allow • Prompt	• Block • Allow

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

Cookie Controls	Chrome 7	Firefox 3.6 / Firefox 4 beta 6	Internet Explorer 8 / 9 Beta	Opera 10.6	Safari 5
First-party cookie default setting	Allowed	Allowed	Allowed	Allowed	Allowed
Global third-party cookie options[19]	• Block • Allow	• Block • Allow • Prompt	• Block • Allow • Prompt • Allow, prompt, or reject as defined in a privacy settings file created by the user	• Accept cookies only from site visited • Allow	• Accept cookies only from sites visited • Allow
Third-party cookie default setting	Allowed	Allowed	Allowed[20]	Allowed	Accept cookies only from sites visited
Granular (per-site) cookie options	• Block • Allow • Session only	• Block • Allow • Session only	• Block • Allow • Prompt • Session only	• Block • Allow • Allow cookies only from site visited • Session only • Prompt	• None

[19] We distinguish between the ability to block/allow all cookies (which is covered by the global first-party cookie option) and the ability to block only third-party cookies.

[20] However, Internet Explorer will block cookies based on their P3P policy. If it does not have a P3P policy, or its policy specifies certain types of use, the cookie is blocked.

Cookie Controls	Chrome 7	Firefox 3.6 / Firefox 4 beta 6	Internet Explorer 8 / 9 Beta	Opera 10.6	Safari 5
Cookie retention options	• Until expiry • Until manually deleted • Until browser is closed	• Until expiry • Until manually deleted • Until browser is closed • Prompt each time	• Until expiry • Until manually deleted • Until browser is closed • As defined in a privacy settings file created by the user	• Until expiry • Until manually deleted • Until browser is closed	• Until expiry
Can prevent deleted cookies from being reset	No	No	No	No	No
Allow lists can be subscribed to	No	No	No[21]	No	No
Block lists can be subscribed to	No[22]	No	No[23]	No	No
Blocking all cookies from being set prevents existing cookies from being read	Yes	Yes	Yes, if set via privacy setting. No if set via advanced controls.	Yes	No
Globally blocking third-party cookies / accepting cookies only from site visited prevents acceptance of third-party cookies	Yes	Yes	Yes	No	Yes

[21] Microsoft has recently announced that it will support block and allow lists in the release version of Internet Explorer 9.

[22] Chrome, however, does support pattern based domain blocking.

[23] Microsoft has recently announced that it will support block and allow lists in the release version of Internet Explorer 9.

Cookie Controls	Chrome 7	Firefox 3.6 / Firefox 4 beta 6	Internet Explorer 8 / 9 Beta	Opera 10.6	Safari 5
Globally blocking third-party cookies / accepting cookies only from site visited prevents existing third-party cookies from being read	No	Yes	No	No	No
Globally blocking third-party cookies / accepting cookies only from site visited prevents first-party cookies from being used as a third-party cookie[24]	No	Yes	No	No	No

[24] An example of this scenario is when the user visits Site A and receives a cookie from Site A. When the user later visits Site B, which happens to have an element from Site A on it, the Site A cookie should not be read and sent to Site A if third-party cookies have been disabled because this cookie is now a third-party cookie.

Object Controls Comparison

Browsers receive and transmit content of many different types – everything from basic text and images to style sheets, scripts, local shared objects ("flash cookies"), and more.[25] When the same objects appear repeatedly across different sites, they can be used to track Internet users. When content is requested from a website, the browser sends information, including the computer's IP address and any cookies associated with the website. Some objects, such as DOM and local shared objects, also allow websites to store information locally even if cookies have been disabled. The comparison below describes browser controls around such objects, plus browser features that can be used to block entire websites from communicating with the browser. The ability for users to create lists of objects to block or allow is also addressed. Some object frameworks, such as Adobe Flash Player, are third party plug-ins. These third party controls are not addressed in this report.[26]

Object Controls[27]	Chrome 6 Beta	Firefox 3.6 / Firefox 4 Beta 6	Internet Explorer 8 / 9 Beta	Opera 10.6	Safari 5
Object types that can be blocked	• Images • JavaScript • DOM storage[28]	• Images • JavaScript	• Images • JavaScript • ActiveX controls[29] • All objects requested from unique domains by third parties (InPrivate Filtering)	• JavaScript • Animated images • Sound • Objects expressible using a filter string or selectable in Opera's GUI interface	• JavaScript

[25] In this report, we refer to all these kinds of content as "objects."

[26] For information on managing Adobe Flash Player, see http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager.html.

[27] This chart examines controls that allow users to block or enable objects other than traditional cookies. Browser controls for traditional cookies are explored above. Although third party extensions may exist that provide object controls, this report focuses only on core browser features.

[28] Chrome includes DOM storage controls under the cookie control settings (Options-> Under the Hood-> Content Settings-> Cookies).

[29] ActiveX controls are supported only by Internet Exporer, so other browsers do not need to block ActiveX.

Object Controls[27]	Chrome 6 Beta	Firefox 3.6 / Firefox 4 Beta 6	Internet Explorer 8 / 9 Beta	Opera 10.6	Safari 5
Objects blocked by default	• None	• None	• None, unless InPrivate Filtering has been enabled.[30]	• None	• None
Users can create exceptions for specific object instances when that object type has been generally blocked/allowed	Yes	Yes, for images.	Yes, for content blocked using InPrivate Filtering.	Yes[31]	No
Object block settings are persistent	Yes	No	No	Yes	No
Supports block lists	No[32]	No	Yes	Yes	No
Supports automatic updating of block lists	No	No	No	No	No
Supports allow lists	No	No	Yes	Yes	No
Supports automatic updating of allow lists	No	No	No	No	No
Controls for DOM storage[33]	• Allow[34] • Disable • Session only	No[35]	• Allow • Disable	• Allow • Disable • Prompt	No

[30] 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. The number of times something must be served or requested defaults to 10, but it can be changed to 3-30.

[31] Opera provides a graphical interface that enables the user to select specific objects to allow/block on a page.

[32] However, Chrome does support pattern based domain blocking.

[33] DOM storage, like HTTP cookies, stores data locally. However, unlike cookies, DOM storage makes it easier for websites to access data shared across sites, and DOM storage supports larger data sets.

[34] Chrome's DOM storage settings are part of their cookie control settings.

[35] Users can disable DOM storage in Firefox by modifying the configuration file using about:config.

Object Controls[27]	Chrome 6 Beta	Firefox 3.6 / Firefox 4 Beta 6	Internet Explorer 8 / 9 Beta	Opera 10.6	Safari 5
Provides a link to Adobe's website Storage Settings panel to manage Flash local storage settings	Yes[36]	No	No	No	No
Controls for other local storage[37]	No	No	No	No	No

[36] Chrome is the only browser that packages Adobe's Flash as part of the browser. However, Adobe's Flash is widely used across all browsers.

[37] This includes controls for components that store information locally, such as Adobe Flash and Microsoft Silverlight.

Geolocation Controls Comparison

Location based services are rapidly becoming more prevalent on the Web. Although websites have attempted to determine geolocation based on IP address for years, such determinations were not very precise. Recent developments have enabled geolocation services to provide precise information about a user's geolocation. Geolocation-enabled browsers use a service provider to obtain the user's estimated geolocation. This information is then provided to websites requesting location information. The chart below compares the geolocation controls available in each of the browsers.[38]

Geolocation Controls	Chrome 7	Firefox 3.6 / Firefox 4.0 Beta 6	Internet Explorer 8 / 9 Beta	Opera 10.6	Safari v5
Geolocation data sharing options	• Prompt (choice is persistent for that site) • Allow all • Block all	• Prompt (can choose to remember choice per site)	IE8 and IE 9 Beta do not support geolocation services	• Prompt (can choose to always/never share per site) • Disable	• Prompt (can choose to re-prompt only once every 24 hours) • Disable
Default for sharing geolocation	Prompt	Prompt	NA	Prompt	Prompt
Prompt identifies the actual site requesting geolocation	Yes	Yes	NA	Yes	Yes
User can grant permission to share geolocation without the decision being persisted	No	Yes	NA	Yes	Limited to 24 hours
Default geolocation service provider	Google Location Service	Google Location Service	NA	Google Location Service	

[38] This comparison only explores controls that are surfaced through the user interface. If the option requires low-level configuration modification, then it is not considered an available control for purposes of this comparison. A common example of this is the geolocation service provider. While this provider can be changed in many of the browsers, it is a setting that requires the user to modify low-level configuration and is not directly surfaced through the interface.

Geolocation Controls	Chrome 7	Firefox 3.6 / Firefox 4.0 Beta 6	Internet Explorer 8 / 9 Beta	Opera 10.6	Safari v5
Geolocation service provider can be changed	No	No	NA	No	No
The geolocation service can be disabled for all geolocation requests	Yes	No[39]	NA	Yes	Yes
The geolocation service can be disabled for third-party content requests	No	No	NA	No	No
Disabling geolocation service prevents sites previously granted persistent permission from receiving geolocation	No	NA	NA	Yes	Yes
Provides an indicator that geolocation is being provided.	Yes	No[40]	NA	Yes	No
The geolocation indicator identifies which sites are receiving geolocation	Yes	NA	NA	No	NA
User can revoke permission for a specific site previously given persistent access to geolocation	Yes	Yes[41]	NA	Yes	No
User can revoke permission for all sites previously given persistent access to geolocation	Yes	No	NA	No	Yes

[39] Users can disable all geolocation requests in Firefox by modifying the configuration file using about:config.

[40] Firefox 4 beta 6 briefly displays an indicator when prompting the user to share. However, the indicator disappears after a decision is made.

[41] The user must navigate to the site that permission was granted for, select Tools-> Page Info, select Permissions, and then deselect Share Location.

Geolocation Controls	Chrome 7	Firefox 3.6 / Firefox 4.0 Beta 6	Internet Explorer 8 / 9 Beta	Opera 10.6	Safari v5
User can grant permission to a specific site that was previously blocked	Yes	Yes[42]	NA	Yes	No
Allow lists can be subscribed to	No	No	No	No	No
Block lists can be subscribed to	No	No	No	No	No
User can view and manage a list of all sites that have been granted/denied geolocation access	Yes	No	NA	No	No

For more information

Please contact:

Justin Brookman
Director, Consumer Privacy Project
(202) 407-8812

[42] The user must navigate to the site that was blocked, select Tools-> Page Info, select Permissions, and then select Share Location.