Mozilla Firefox Privacy Policy

Last Updated: November 31, 2010

Prior Policies **[insert link to new page where all previous desktop and mobile privacy policies should be posted, including versions from January 2010 and any other policies we have]**

This privacy policy explains how Mozilla Corporation ("Mozilla"), a wholly-owned subsidiary of the non-profit Mozilla Foundation, collects and uses information about users of the official Mozilla Firefox® web browser ("Firefox"). It does not apply to other Mozilla websites, products, or services.

Overview

In this privacy policy, we address the following:

*Definitions of the types of information
*What Firefox Sends to Websites
*Feature-by-Feature Description of Data Practices
*What Mozilla Does to Secure Data
*Government and Court Demands for Information
*Overview of Other Situations Involving Possibility of Data Disclosures
*Mozilla's Approach to Data Retention
*How Mozilla Discloses Changes to this Policy
*How to Contact Mozilla about this Policy
*Appendix of Practices relating to Prior Versions of Firefox

Types of Information

"Personal Information" is information that you provide to us that personally identifies you, such as your name, phone number, or email address. Except as described below, Mozilla does not collect or require end-users of Firefox to provide Personal Information.

"Non-Personal Information" is information that cannot be directly associated with a specific person or entity. Non-Personal Information includes but is not limited to your computer's configuration and the version of Firefox you use.

"Potentially Personal Information" is information that is Non-Personal Information in and of itself but that could be used in conjunction with other information to personally identify you. For example, Uniform Resource Locators ("URLs") (the addresses of web pages) or Internet Protocol ("IP") addresses (the addresses of computers on the Internet), which are Non-Personal Information in and of themselves, could be Personal Information when combined with Internet service provider ("ISP") records.

"Aggregate Data" is information that is recorded about users and collected into groups so that it no longer reflects or references an individually identifiable user.

Information Firefox Sends to Websites and ISPs

Like other web browsers, Firefox sends Non-Personal and Potentially Personal Information to the websites you visit when requested by the website. This may include, e.g. the type of browser you are using, the type of device you are using (desktop, mobile, touch screen), your language preference, the referring site, and your IP address. If you are viewing a video, the buffering functionality of Firefox may allow the server hosting the video to determine which sections of the video you have actually played. This information may be logged by the websites you visit and the Internet Service Provider you are using. What information is logged and how that information is used depends on the policies of each of the websites you visit and the ISPs you use.

Each website determines its own privacy practices for the distribution and use of this Non-Personal Information and Potentially Personal Information. If you are concerned about how a website will use this information, check out its privacy policy. To find out more about how Mozilla uses this information on its own websites, see the Mozilla Privacy Policy.

Cookies

A cookie is information stored on your computer by a website you visit. Cookies often store your settings for a website, such as your preferred language or location. When you return to the site, Firefox sends back the cookies that belong to the site. This allows the site to present you with information customized to fit your needs. Cookies can store a wide range of information, including personally identifiable information (such as your name, home address, e-mail address, or telephone number). Because of their ability to store Personal Information, or references to such information, cookies can allow websites to track the online movements of particular individuals.

Firefox itself does not set any cookies on behalf of Mozilla.

By default, the activities of storing and sending cookies are invisible to you. However, you can change your Firefox settings to allow you to approve or deny cookie storage requests, delete stored cookies automatically when you close Firefox, and more. An article in our Firefox Knowledge Base gives you information about changing these preferences.

SMS Text Message Downloading **(Firefox for mobile only)**

In addition to downloading Firefox for mobile onto your mobile device from our download website, Mozilla provides an easy way to send yourself an SMS text message from the Firefox for mobile main website, which will include a download link. If you choose to send a text message, the mobile phone number you type into the box on the website will not be stored on any Mozilla servers.

Interactive Product Features

***Add-ons Features*.** One thing that makes Firefox so flexible is the ability for you to add various add-ons, extensions, and themes to Firefox, thereby creating a custom browser that fits your needs. The following features show how Firefox provides the ability both to obtain additional add-ons easily and to protect against potentially harmful add-ons.

Get Add-ons Page

Firefox offers a Get Add-ons page of the Add-ons Manager that features popular add-ons and displays personalized recommendations based on the add-ons you already have installed. This page can be accessed by clicking (or tapping on a mobile device) on the "Get Add-ons" tab of the Firefox Add-ons Manager. To display the personalized recommendations, Firefox sends certain information to Mozilla, including the list of add-

ons you have installed, Firefox version information, and your IP address. This communication only happens when the Get Add-ons area is open and can be turned off at any time by opting out of Automatic Updates from the Add-ons Manager.

Add-on Information and Searches

In order to keep the information displayed to you about your installed add-ons up to date, Firefox communicates with Mozilla once a day to update add-on descriptions, home pages, download counts, screenshots, and ratings. This communication includes the list of add-ons you have installed, Firefox version information, and your IP address. You can turn off this functionality at any time by opting out of Automatic Updates from the Add-ons Manager.

If you enter keywords into the search field for the Add-ons Manager, those keywords will be sent to Mozilla in order to perform the search, along with Potentially Personal Information (such as IP address) normally transferred to perform such functionality.

***Automated Update Service*.** Firefox's automatic update feature periodically checks to see if an updated version of Firefox and installed add-ons are available from Mozilla.

This feature sends Non-Personal Information to Mozilla, including the version of Firefox you are using, build ID and target, update channel, your language preference, and your operating system. This feature also sends Potentially Personal Information to Mozilla in the form of your IP address and a cookie that contains a unique numeric value to distinguish individual Firefox installs. Mozilla uses this information to provide you with updated versions of Firefox and to understand the usage patterns of Firefox users. We use this information to improve our products and services and to support decision making regarding feature and capacity planning.

Mozilla does not collect or track any Personal Information or any information about the websites you visit, and Mozilla does not release the raw information we obtain from these Firefox features to the public. We may release reports containing Aggregate Data so that our global community can make better product and design decisions. To prevent Mozilla from obtaining this information, you can turn this feature off in Firefox's preferences. An article in our Firefox Knowledge Base gives you information about changing your preferences in non-mobile versions of Firefox.

***Blocklist Feature*.** Firefox also offers a Blocklist feature. With this feature, once a day Firefox does a regularly scheduled, automatic check to see if you have any harmful add-ons or plug-ins installed. If so, this feature disables add-ons or plug-ins that Mozilla has determined contain known vulnerabilities or major user-facing issues or fatal bugs (e.g., Firefox crashes on startup or something causes an endless loop). You may view the current list of Blocklisted items. This feature sends Non-Personal Information to Mozilla, including the version of Firefox you are using, operating system version, build ID and target, update channel, and your language preference. This feature also sends Potentially Personal Information to Mozilla in the form of your IP address and a cookie. In addition, Mozilla also uses this feature to analyze Firefox usage patterns so we may improve our products and services, including planning features and capacity. Currently there is no basic user interface to disable the Blocklist feature. An article in our Firefox Knowledge Base explains how you may disable the Blocklist feature. Disabling the Blocklist feature is not recommended as it may result in using extensions known to be untrustworthy.

***Crash-Reporting Feature*.** Firefox for computers (not the mobile version) has a crash-reporting feature that sends a report to Mozilla when Firefox crashes. Mozilla uses the information in the crash reports to diagnose and correct the problems in Firefox that caused the crash. Though this feature starts automatically after Firefox crashes, it does not send information to Mozilla until you explicitly authorize it to do so. By default, this feature sends a variety of Non-

Personal Information to Mozilla, including the stack trace (a detailed description of which parts of the Firefox code were active at the time of the crash) and the type of computer you are using. Additional information is collected by the crash reporting feature. Which crash reporting feature is used and what additional information collected by Firefox depends on which version of Firefox you're using. For pre-3.x versions of Firefox, please see the end of this privacy policy.

Firefox 3.0 to present

For the current versions of Firefox, "Firefox Crash Reporter" is Firefox's crash reporting feature. With this feature, you have the option to include Personal Information (including your email address), Potentially Personal Information (including your IP address and the URL of the site you were visiting when Firefox crashed), and a comment. Firefox Crash Reporter also sends a list of all add-ons that you were using at the time of the crash, the time since (i) the last crash, (ii) the last install, and (iii) the start-up of the program. For Firefox 3.0.0 – 3.0.5, Firefox Crash Reporter also collects Potentially Personal Information to Mozilla in the form of a unique alphanumeric value to distinguish individual Firefox installs. This value is not assigned to users of Firefox 3.0.6 and subsequent versions. Mozilla only makes Non-Personal Information (i.e., generic information about your computer, the stack trace, and any comment given by the user) available in the public reports available online at http://crash-stats.mozilla.com/.

***Location-Aware Feature*.** Beginning with Firefox 3.5 and all versions of Firefox for mobile, Firefox offers a Location-Aware Feature, parts of which may be provided by third-party service providers.

You Elect to Use the Location-Aware Feature

This feature remains inoperative until you visit a website that requests your location and you choose to opt in to the feature. If you elect not to, nothing happens. Each time you visit such a website, Firefox asks you if you want it to provide the site with your current location. Additionally, you may elect to have Firefox remember your choice to allow or not allow the feature for each site. Any such election is domain specific. You are able to opt out at any time of having Firefox remember your choice, just like any other preference setting.

What Information Firefox Collects

If you choose to allow it, the Firefox Location-Aware Feature first collects one or more of the following relevant location markers: (i) location provided by a GPS device built into or attached to your computer or device and/or geolocation services provided by the operating system; (ii) the wifi routers closest to you; (iii) cell ids of the cell phone broadcast towers closest to you; (iv) the signal strength of nearby wireless access points and/or cell phone broadcast towers; and/or (v) your computer or device's IP address. Next, it attempts to determine your location using these location markers. Any information Firefox uses, receives or sends as part of this Location-Aware Feature is not received by any Mozilla servers or by Mozilla. Firefox does not track or remember your location. Firefox does remember a random client identifier, the temporary ID assigned by our third party provider to process your request, for two weeks.

Transmission of Geolocation Information to Third Parties

If your computer or device has a GPS unit or your operating system provides geolocation services and you have elected to use the location aware feature, Firefox will send your location information directly to the requesting website. If not, Firefox will send the other information described above, plus your user agent information (e.g., version of Firefox you're using) and a temporary client identifier, to a third party geolocation services provider. That provider can determine your approximate location from such data (e.g., convert a set of WiFi signal strengths into latitude and longitude). This information is sent by Firefox over an encrypted connection and no cookies are used. Neither the domain

name nor the URL of the site you're visiting is sent to our service providers. Our providers estimate your location and return it to Firefox. Firefox provides your location information to the webpage that made the request.

Restrictions on How Third Party Providers Use the Location Information Received

Our policy is to require third-party providers to enter licensing agreements with Mozilla, which prohibit them from releasing Personal or Potentially Personal Information to the public. We only permit our third party providers to use this information in conjunction with the service(s) they are providing to us. They are required to ensure that any information collected on our behalf is anonymized and aggregated before they are permitted to use such information to develop new features or products and services, or to improve the overall quality of any of their products and services. For example, this means that they are required to ensure that your IP address and unique identifier of your client will be stripped out before being used by any of our third party provider's other products or features. For more information on how our geolocation services providers use information sent by Firefox, please see the privacy policy links in our list of third-party service providers.

Third Party Privacy Policies

Please carefully consider any website or service provider's privacy practices before agreeing to share your location.

- *Requesting Websites*. For information on the use of location data sent back to the website, please see that website's privacy policy.
- *Location-Aware Service Providers*. For information on how our service providers use the location data sent by Firefox, see theprivacy policies linked from our list of third-party service providers.

Panorama Feature. Starting with Firefox 4 (not applicable to Firefox for), Firefox provides Panorama, which manages your tab experience. Your tab usage and names are not sent to Mozilla, but rather reside locally on your device. The first time you run Panorama, a video may be presented to you explaining Panorama. The video or web page is hosted by Mozilla so Mozilla receives your IP address and date and time of receiving the video.

***Firefox Sync Feature*.** The Firefox Sync feature is included in versions of Firefox beginning with Version 4. Firefox Sync allows you to synchronize certain data between your computers, mobile phones, and other devices that have the Firefox browser installed, by utilizing the Firefox Sync Services. (You can also use Sync with a syncing service hosted on a non-Mozilla server set up by yourself or a third party, but in that case this policy doesn't apply to your use of such syncing service.) Examples of data you can synchronize include browsing history, form history, bookmarks, saved passwords, preferences, and open tabs. This data ("Firefox Sync User Data") is stored on, manipulated, and transmitted to and from Mozilla's servers by means of your use of the Firefox Sync Services. Firefox Sync User Data is encrypted on your computer before it is sent to Mozilla's servers, so it is not available to Mozilla in a readable form. Mozilla uses SSL/TLS technology to ensure your Firefox Sync User Data is encrypted during transit.

In order to utilize the Sync functionality you must register for the Firefox Sync Services. During registration you will need to provide your email address and create a username and password (collectively "Account Data"). Your Account Data will be encrypted using SSL/TLS for transit. Your password will be stored on our servers in an encrypted form called a hash. This form of encryption disguises your password on the server, but still allows us to authenticate you when you sign into the Firefox Sync Services. Certain versions of Sync also ask you to create a secret phrase. The secret phrase is stored on your computer and is not sent to the Firefox Sync servers or to Mozilla. Mozilla does not collect any other Personal Information through Firefox Sync.

Mozilla receives and uses the following Non-Personal and Potentially Personal Information for the purpose of providing and improving the Firefox Sync Services: IP address, username, date and time of accessing the Firefox Sync Services, user agent string information such as the type of client OS and Firefox version in use, and aggregated operational data such as access log data and how many bookmarks, history, or tabs users have collectively created and synced.

The Firefox Sync Services also receive the host names you have given your devices that you are syncing. These names are used to label your tabs within Firefox Sync. If you don't want to share your devices' names, you should consider naming your devices with fanciful names rather than your actual name. The information is transmitted using SSL. Currently, you can opt out of having your devices named in Firefox Sync by visiting the Firefox preferences pane or about:config.

You can disconnect from the Firefox Sync Services and have your Account Data and Firefox Sync User Data removed from our servers at any time. On your computer, go to the "Tools" menu, highlight "Sync," and click "Disconnect." Then go to https://services.mozilla.com/delete-account/, and submit the form to request deletion of your Account Data and Firefox Sync User Data from our servers. If you are transferring a synced device to another party (such as if you are sharing, reselling, or donating your laptop or phone) you may wish to disconnect and then remove your Sync data from your device to avoid sharing it with the device recipient.

***Personas Feature*.** Firefox's Personas feature is a theme that lets you personalize the look of your browser (not currently applicable to Firefox for mobile).

Applying Personas

When you apply a Persona to your browser, Mozilla collects your IP address, the date and time you applied the Persona to your browser, and the url you used to make the application as well as the url you were visiting immediately before that (known as the "referrer" url).

Creating a Custom Persona

If you are creating a Custom Persona for your own use, Mozilla does not collect any Personal Information.

Contributing a Design to the Personas Gallery

The Personas gallery is where you can browse all the available designs. If you contribute a design or image (each a "Persona") to the Personas gallery, Mozilla collects the following Personal Information: (1) your username and (2) your email address. Your username will be used to attribute your Persona to you and will be publicly available on the Personas gallery. You do not have to provide your real name; you can use a nickname or avatar. Mozilla will not make your email address publicly available without your consent or share it with any third parties other than Mozilla's service providers. Mozilla will use your email address only to contact you regarding your design or to provide any additional information that you elect or opt in to receive.

Personas' Interactive Product Features

After you have selected your Persona, it is stored on your computer. Once per day the Personas service checks to see if your selected Persona has been updated. This feature sends the same information that web browsers typically transfer with any HTTP requests including user agent and your IP address.

We use this information to improve our products and services and to support decision making regarding feature and capacity planning. Mozilla is an open organization that believes in sharing as much information as possible about its products, its operations, and its associations. Accordingly, we may release public reports containing Aggregate

Data so that our global community and Personas partners may make better product and design decisions. For example, we think it is good for users of Personas to know which are the most popular Personas and Personas designers to know how many times their Persona was downloaded.

Report Web Forgery Feature (not applicable to Firefox for mobile). Firefox's Report Web Forgery feature lets you report suspected web forgeries to Mozilla's third party service provider(s) for the web forgery protection feature when you encounter a suspected malicious "phishing" or fraudulent website that is impersonating a legitimate website. This feature sends your comments about the suspected fraudulent website to our third-party provider(s), as well as the same information that the browser sends when you visit a website. Our policy is to require each of our third-party providers to enter into written agreements with Mozilla that prohibit them from releasing Potentially Personal Information to the public. Our policy is to only permit these third party providers to use this information in conjunction with the web forgery protection service they are providing. In addition, we require each third-party provider to maintain its own privacy policy that is linked to the online form where you report a potential web forgery. To prevent the third party provider from obtaining this information, don't use this feature to report a web forgery. (Also see *"Protection Against Suspected Forgery and Attack Sites Features"* below.)

Feedback Button and Test Pilot for Beta Users (not applicable to the mobile version). If you installed the Firefox 4 beta and then got Firefox 4 by clicking an "update" button, then your Firefox still has the feedback features you received as a beta user. If you installed the Firefox 4 beta and then got Firefox 4 by clicking a "download" button, you still have the Test Pilot add-on as an extension to Firefox. The privacy policy for Feedback and Test Pilot are here. If you decide to remove Test Pilot or Feedback, you can do so under the Tools menu in Firefox by selecting add-ons in the drop down menu and then uninstall.

Security

Mozilla is committed to protecting your personal information from unauthorized access, alteration, disclosure, or destruction. We undertake a range of security measures including physical access restraints, technical security monitoring, and internal security reviews of the environment. We also have policies in place to prohibit employees from viewing personal information without business justification. Additionally, it is our policy to ensure that Mozilla employees and contractors are bound by confidentiality obligations.

Beginning with Firefox 2.0, Mozilla has additional security features, some of which are provided by third-party service providers.

The security features available depend on the version of Firefox you are using. Please see the end of this privacy policy for older versions of Firefox.

Firefox 3.0 to Present

Secure Website Certificate Verification. When you visit a secure website, Firefox may check with any status provider mentioned in the certificate to validate that website's certificate. Firefox sends only the certificate identification to the certificate provider, not the exact URL you are visiting. Sending these verification requests to third parties is sometimes necessary to ensure your connection to a site is secure; to help maintain your security, Firefox may block access to the site if it can't verify your connection using the third party. If the certificate is no longer valid, you will receive an error page that states why the certificate is not valid and you will not be able to access that website. The technical name for this process is OCSP or On-line Certificate Status Protocol. You may disable online certificate verification in Firefox's preferences under the encryption tab. If you do this, none of the information discussed here will be sent to any third

party certificate provider. An article in our Firefox Knowledge Base gives you information about changing your preferences. However, if you choose to disable the online verification feature, Firefox will not be able to confirm the identity of the website you are visiting, which may put you at greater risk of having your private information intercepted. In this case, Firefox will also not show the identity of the website in the URL bar.

Protection Against Suspected Forgery and Attack Sites Features (not applicable to Firefox for mobile). The Firefox forgery and attack protection feature displays a warning if the website you are visiting is suspected of impersonating a legitimate website (commonly referred to as a phishing or forgery website) or a site that infiltrates or damages a computer system without your informed consent, including, without limitation, any computer viruses, worms, trojan horses, spyware, computer contaminant and/or other malicious and unwanted software (commonly called an attack site or malware). By default, Firefox checks the web pages that you visit against a blacklist that is downloaded to your hard drive at regularly scheduled intervals (e.g., approximately twice per hour), the rate of frequency may change from time to time. The blacklist does not include the full URL of each suspicious site. Instead, each URL is hashed (obscured so it can't be read) and then broken into portions. Only a portion of each hashed URL is included on the blacklist on your hard drive. If there is a match, Firefox will check with its third party provider to ensure that the website is still on the blacklist. The information sent between Firefox and its third party provider(s) are hashed URLs. In fact, multiple hashed URLs are sent with the real hash so that the third party provider(s) will not know what site you are visiting. If there is a match, Firefox displays either a "Reported Web Forgery" or "Reported Attack Site" alert, as applicable.

You may completely turn off the forgery and/or attack site protection features in Firefox's preferences. If you do this, none of the information discussed here will be downloaded to your hard drive or sent to any third party service provider. An article in our Firefox Knowledge Base gives you information about changing your preferences.

Each time Firefox checks in with a third party provider to download a new blacklist, Non-Personal Information and Potentially Personal Information, such as the information that the browser sends every time you visit a website as well as the version number of the blacklist on your system, is sent to a third party provider. In order to safeguard your privacy, Firefox will not transmit the complete URL of web pages that you visit to anyone other than Mozilla and its service providers. While it is possible that a third party service provider may determine the actual URL from the hashed URL sent, Mozilla's policy is to require its third party service providers to enter into a written agreement with Mozilla not to use any data or other information about or from users of Firefox for purposes other than to provide and maintain their service. In addition, Mozilla's policy is to prohibit these third party service providers from correlating any Firefox user data with any other data collected through other products, services or web properties of that provider. These third party service providers may post about additional notices regarding their applicable privacy policies. (For example, see Google Safe Browsing Service in Mozilla Firefox Version 3.)

Please note that we're not yelling at you in this paragraph. Our lawyers have advised us that we need to make sure this information is conspicuous so you'll read it. **The forgery and attack site protection feature is provided "as is" and for your information as advice and guidance only. Mozilla and its contributors, licensors and partners do not guarantee that these protection features will prevent you from being deceived by a malicious website and we strongly recommend that you continue to be vigilant while online, particularly when following links sent to you in e-mail.**

Government and Court Demands for Information

Mozilla may be required to disclose information to the government or others. This may happen if we receive a valid search warrant, subpoena, court order, or other legal mandate. For example,

the DMCA framework (specifically in Section 512(h)) contains an expedited subpoena process for copyright holders to request and receive information service providers have regarding the identity of alleged copyright infringers.

Other Disclosures

In certain other limited situations, Mozilla may disclose your Personal Information, such as when necessary to protect our websites and operations (e.g., against attacks); to protect the rights, privacy, safety, or property of Mozilla or its users; to enforce our terms of service; and to pursue available legal remedies. Additionally, Mozilla may need to transfer Personal Information to an affiliate or successor in the event of a change of our corporate structure or status, such as in the event of a restructuring, sale, or bankruptcy.

What and When We Share with Third Parties

Mozilla's policy is to make Personal Information, such as your name and email address, and Potentially Personal Information, such as the URL of the site you last visited, only available to its employees, contractors, and selected contributors who signed confidentiality agreements that prohibit them from using or disclosing such information other than for approved Mozilla purposes.

We also work with third parties who provide infrastructure or back-end services (like content delivery networks, bandwidth providers, and services of an administrative nature). We may share Personal Information about you with such third parties for the purpose of enabling these third parties to provide such services.

Transfer of Data to the U.S.

Mozilla is a global organization and operates in different countries. Privacy laws and common practices vary from country to country. Some countries may provide for less legal protection of your personal data; others may provide more legal protection. By using Firefox, you consent to the transfer of the information collected, as outlined by this Policy, to Mozilla or its third party service providers in the United States, the Netherlands, and other places where our distributed, third party content delivery network exists (which is in several countries around the world), which countries may provide a lesser level of data security than in your country of residence.

Data Retention

We will retain any information collected for the period necessary to fulfill the purposes outlined in this Policy unless a longer retention period is required by law and/or regulations.

Privacy Policy Changes

Mozilla may change the Firefox Privacy Policy from time to time. Any and all changes will be reflected on this page. Substantive changes may also be announced through the standard mechanisms by which Mozilla communicates with its users and community, such as Mozilla's "announce" mailing list and newsgroup. It is your responsibility to ensure that you understand the terms of this Privacy Policy. You should periodically check this page for any changes to the current policy.

For More Information

You may request access, correction, or deletion of Personal Information or Potentially Personal Information, as permitted by law. We will seek to comply with such requests, provided that we have sufficient information to identify the Personal Information or Potentially Personal Information related to you.

Any such requests or other questions or concerns regarding this Policy and Mozilla's data protection practices should be addressed to:

Mozilla Corporation
Attn: Legal Notices - Privacy
650 Castro Street, Suite 300
Mountain View, CA 94041-2072
Phone: +1-650-903-0800
E-mail: privacy@mozilla.com

Appendix for Pre-Firefox 4.0

Report Broken Website Feature. -3.6.x.

Firefox's Report Broken Website feature lets you notify Mozilla when a website you visit improperly displays or incorrectly functions. The feature sends the URL of the broken website to Mozilla. You may also choose to send your email address and a description of the problem. This feature also sends your IP address and a variety of Non-Personal Information to Mozilla, including but not limited to the version of Firefox you are using and your language preference. Except for your email and IP address, Mozilla makes all of this information public. This feature does not send information to Mozilla until you explicitly authorize Firefox to do so. To prevent this public release of Personal and Potentially Personal Information, don't report a website if the website's URL contains your Personal and Potentially Personal Information, and don't include Personal Information in your description of the problem. To prevent the release of any information, don't use this feature to report a broken website.

Crash-Reporting Feature for Firefox 1.0-2.x.

For these earlier versions of Firefox, "Talkback" is Firefox's crash reporting feature. Talkback also gives you the option to provide your Personal Information and Potentially Personal Information (including your name, email address, and the url you were visiting) and Potentially Personal Information (including your computer's name, IP address, and the processes you were running at the time of the crash). You can selectively disable the sending of this information. Additionally, you have the option to include the URL of the site you were visiting when Firefox crashed, a comment, and your email address in the report. Mozilla only makes Non-Personal Information and Potentially Personal Information in the public reports available online at http://talkback-public.mozilla.org/.

Security for Firefox 2.0 to 2.x.

Protection Against Suspected Forgery Sites. The Firefox web forgery protection feature displays a warning if the website you are visiting is suspected of impersonating a legitimate website. Firefox lets you select various levels of protection, and different information is transmitted by Firefox depending on the level you choose.

By default, Firefox checks the web pages that you visit against a list of suspected web forgeries (a "blacklist") that is downloaded to your hard drive at regularly scheduled intervals (e.g., approximately twice per hour), the rate of frequency may change from time to time. If there is a match, Firefox displays a "Suspected Web Forgery" alert. Each time Firefox checks in with the third party provider to download a new blacklist, Non-Personal Information and Potentially Personal Information, such as the information that the

browser sends every time you visit a website as well as the version number of the blacklist on your system, is sent to the third party provider. In order to safeguard your privacy, Firefox will not transmit the URL of web pages that you visit in this default mode to anyone other than Mozilla and its service providers.

You may completely turn off the web forgery protection feature in Firefox's preferences. If you do this, none of the information discussed here will be downloaded to your hard drive or sent to any third party service provider.

Each time Firefox checks in with the third party provider to download a new blacklist, Non-Personal Information and Potentially Personal Information, such as the information that the browser sends every time you visit a website as well as the version number of the blacklist on your system, is sent to the third party provider. In order to safeguard your privacy, Firefox will not transmit the complete URL of web pages that you visit to anyone other than Mozilla and its service providers. While it is possible that a third party service provider may determine the actual URL from the hashed URL sent, Mozilla's policy is to require its third party service providers to enter into a written agreement with Mozilla not to use any data or other information about or from users of Firefox for purposes other than to provide and maintain their service. In addition, Mozilla's policy is to prohibit its third party service providers from correlating any Firefox user data with any other data collected through other products, services or web properties of that provider. These third party service providers may inform you about additional notices regarding their applicable privacy policies.