

Submitted Via Email: ec.sen@aph.gov.au

15 December 2010

Stephen Palethorpe
Committee Secretary
Senate Standing Committee on Environment and Communications

We want to thank the Senate Standing Committee on Environment and Communications for the opportunity to respond to the submission from the Australian Privacy Foundation as it relates to Firefox.

Mozilla's interest in this inquiry stems from our identity. We are a global community of people working together since 1998 to build a better Internet. Mozilla and its contributors make technologies for users and developers, including the Firefox web browser used by more than 400 million people worldwide. As a non-profit organization, we are dedicated to promoting openness, innovation, and opportunity online. Thus, we care deeply about user privacy and users' ability to control their data and identity online.

We would like to address the APF's comment about Firefox. However, it is not clear from the APF submission what they are referencing. In the absence of further detail, we are unable to comment on the concern. We would be happy to engage in further discussion about the issue once we are provided specific details.

Until then, we would like to take this opportunity to discuss Mozilla's privacy practices more broadly. Mozilla has led in the privacy space on a number of levels. In the spring, Mozilla's engineers were the first to fix a long-standing CSS bug that affected all browsers and allowed websites to determine whether a user had been to a particular website. Mozilla's groundbreaking fix to this problem is now integrated into our current beta releases and our upcoming Firefox 4.0 product. Our fix was well documented, publicly discussed, and available to other vendors and the public under an open source license. We were glad to see that, after sharing this publicly, other browser vendors fixed the bug in their products as well. Mozilla was proud of its ability to move the industry on this important privacy issue.

Firefox has seen a number of other privacy-enhancing features added recently. These include private browsing mode, clear recent history, forget about this site, and a privacy-sensitive implementation of geolocation that requires users to opt-in before geolocation data is sent to websites, doesn't share the url of the site with the location-based service provider, and requires those service providers to send location data encrypted. You can see an overview of privacy and security features in Firefox here: <http://www.mozilla.com/en-US/firefox/features/#security>

Mozilla is similarly proud of its other products, such as Firefox Sync (aka Firefox Home on the iPhone), which utilizes privacy best practices. This product allows a

user's browsing experience (tabs, bookmarks, history, passwords) to be consistent across multiple devices. Mozilla designed the product so that this web data is encrypted, and users exclusively have the tools to decrypt it.

We also have designed our user studies software, TestPilot, so that users are given notice in a real-time and conspicuous manner before a study begins and must opt-in before their test results are submitted to Mozilla. And users can view the full set of raw data before deciding whether to submit their data to us. And, by default, the users must separately opt-in to their results being included for each study. Additionally, TestPilot is either downloaded expressly by the user or is part of beta packages that target users looking to help Mozilla improve its products.

At Mozilla, designing products in a privacy-sensitive manner is an ongoing process, and we look forward to continuing to innovate in this area so that users can better control their data and their web experience.

Respectfully Submitted,

Mozilla

/s/ Julie Martin

Julie Martin, Associate General Counsel