Why Private Browsing Modes Do Not Deliver Real Privacy*

Christopher Soghoian
Center for Applied Cybersecurity Research, Indiana University
chris@soghoian.net

> "Thanks to Private Browsing, Safari doesn't save or cache any personal information you enter or pages you visit. *It's as if you were never there.*" [8]
>
> "[Firefox] Private Browsing: Surf the Web *without leaving a single trace.*" [3]

Over the past few years, all of the major web browser vendors have embraced the concept of Privacy Enhancing Technologies (PETs), and added "private browsing" modes to their products. Publicly, the companies describe this feature as useful for consumers "shopping for a gift on a family PC" [14] or someone wishing to "to plan surprises like gifts or birthdays" [7].[1]

The private browsing features are widely promoted, and have even been featured in TV advertising campaigns [12, 13]. Unfortunately, the browser vendors have adopted a very narrow threat model of attacks from which they will protect users.[2]

Private browsing modes primarily protect users from a local adversary, who sits down at a user's computer, and attempts to look through their browsing history. Most importantly, the private browsing modes are not intended to effectively protect users from online tracking by third parties [4], from adversaries with access to or control over the user's network connection, such as their ISP or employer, or from a motivated attacker (e.g. a suspicious spouse) willing to install spyware on their computer.

When a user initiates a private browsing session, each of the browsers display some form of text dialog to users. This text details the kinds of data, such as cookies and browsing history that are not retained when the feature is in use. Two browsers, Firefox and Chrome even go so far as to attempt to explain some of the limitations of their respective private browsing modes, and list the kinds of adversaries from which the user is not protected.[3]

Unfortunately, as with many browser warnings [15, 5], it seems pretty clear that consumers are ignoring this text, and therefore it is not possible for them to understand the limitations of private browsing mode. One example that illustrates that users are unaware of the limitations of private browsing comes directly from Mozilla. Despite the fact that "private browsing" does not protect employees from network surveillance conducted by their employers, Mozilla recently reported that the highest use of private browsing mode occurs between 11am and 2pm [17], during typical lunch break hours. Thus, it seems that employees are using the private browsing function included in the Firefox browser, expecting that it will keep the information they are transmitting over their empoloyers networks from the surveillance conducted by their employers, even though Firefox warns users that this threat is specifically not covered.

To be clear, it is not that the private browsing mode features are broken – on the contrary, the browser vendors are for the most part delivering exactly what they claim to deliver. The problem is that consumers do not understand the many limitations of the private browsing mode. Furthermore, because most consumers do not fully understand many forms of online tracking or surveillance [11, 10, 16], offering a private browsing mode may give them a false sense of confidence and encourage them to engage in behaviors they would otherwise avoid (e.g., using a corporate network to view non-work related content during their lunch break).

The fact that consumers are ill equipped to understand the limitations of the private browsing modes makes the marketing of these privacy features highly problematic, since users are therefore likely to believe these features deliver far more actual privacy than they really do, simply based on the name of the feature. One solution to this might be to rename these features to more accurately describe what they actually deliver. Unfortunately, "protect yourself from mildly inquisitive local attackers who

*Position Paper for IAB Internet Privacy Workshop, Boston, MA, December 2010.

[1] The authors of one study of user behavior argue that "the browser vendors may be mischaracterizing the primary use of the feature when they describe it as a tool for buying surprise gifts." Their study found that the primary use of the private browsing feature is actually to look at porn sites [1]. As such, it is not too surprising that the average length of a private browsing session is just 10 minutes [17].

[2] "Private browsing mode is about preventing local traces, not protecting against remote tracking. There are *tons* of ways for a determined host with which you are interacting to track your identity. Apart from protecting against omniscient (government) tracking, the suggested solution is Tor." Statement of Brendan Eich, Mozilla CTO, May 28, 2010 [6].

[3] Google's Chrome should be praised for having by far the clearest yet informative text which is displayed each time the user enters incognito mode.

aren't motivated enough to install spyware on your computer mode" doesn't exactly roll off the tongue.

A more comprehensive solution would be for the browser vendors to actually deliver the kind of privacy protections that many users reasonably expect that the private browsing modes *already* deliver.[4] However, as I will now briefly argue, many of the browser vendors have a strong incentive to not ship effective, comprehensive privacy features in their products.

No incentive to deliver effective privacy enhancing technologies

Many of the browser vendors have worked very hard to earn the trust and support of IT departments, since many users are not often able to install software of their own choosing on their work or university supplied computer. As such, the browser vendors are loath to do anything to upset this relationship. For example, if a browser vendor opts to include technology in their respective browser that is specifically designed to allow users to evade monitoring software or web filters installed by schools and employers, the browser vendor will soon find their product removed from desktops by IT departments, and replaced with a competing browser that lacks such privacy enhancements.

Another incentive problem relates to the fact that the web browsers that consumers use are often made by advertising firms. That is, both Internet Explorer and Chrome, which make up the majority of the PC and smart-phone markets are made by online advertising companies (Google and Microsoft).

Earlier this year, the Wall Street Journal published an expose of the internal deliberations over Internet Explorer's InPrivate Filtering feature, which, when enabled, blocks access to many third party servers, including behavioral advertising networks [18]. As the Journal revealed, Microsoft's online advertising division was able to force the Internet Explorer team to change this feature to be disabled by default. Because most users never change their software defaults [9], the end result of this was to expose millions of consumers to online tracking by behavioral advertising companies, including Microsoft's Atlas Solutions division, who would have otherwise have been protected had the feature been enabled by default.

As the Wall Street Journal's expose so clearly demonstrated, some browser vendors may be unwilling to put users' privacy first, if doing so will impact the profit margins of their advertising divisions.

[4]Mozilla is currently considering the possibility of offering an anonymous browsing mode, that would seek to protect users from a far more expansive list of privacy threats than the current private browsing mode [2].

Conclusion

As I have argued in this brief position paper, private browsing modes currently deliver little meaningful privacy to end users. Furthermore, the browser vendors are unlikely to build strong, privacy enhancing features into their browsers that enable considers to effectively protect themselves from online tracking by behavioral advertising networks, or network surveillance by employers and universities. Unfortunately, many users are likely to reasonably believe that "private browsing" modes deliver just that: *privacy*. Such users may put themselves at risk and engage in risky online behavior that they might otherwise not, if they fully understood the limitations of the browser vendors' chosen threat model.

References

[1] Gaurav Aggrawal, Elie Bursztein, Collin Jackson, and Dan Boneh. An analysis of private browsing modes in modern browsers. In *Proc. of 19th Usenix Security Symposium*, 2010.

[2] Mozilla Corporation. Anonymous Browsing, 2010. `wiki.mozilla.org/Security/Anonymous_Browsing`.

[3] Mozilla Corporation. Firefox Features, 2010. `www.mozilla.com/en-US/firefox/features/`.

[4] Peter Eckersley. How unique is your web browser? In Mikhail Atallah and Nicholas Hopper, editors, *Privacy Enhancing Technologies*, volume 6205 of *Lecture Notes in Computer Science*, pages 1–18. Springer Berlin / Heidelberg, 2010.

[5] Serge Egelman, Lorrie Faith Cranor, and Jason Hong. You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In *CHI '08: Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems*, pages 1065–1074, New York, NY, USA, 2008. ACM.

[6] Brendan Eich. Comment left in Bug #575230: Provide option to reduce precision of Date(), 2010. `bugzilla.mozilla.org/show_bug.cgi?id=575230#c1`.

[7] Google. Google Chrome Help: Incognito mode (private browsing), 2010. `www.google.com/support/chrome/bin/answer.py?hl=en&answer=95464`.

[8] Apple Inc. Safari Features, 2010. `www.apple.com/fr/safari/features.html`.

[9] Jay P. Kesan and Rajiv Shah. Setting Software Defaults: Perspectives from Law, Computer Science and Behavioral Economics. *Notre Dame Law Review, Vol. 82, pp. 583-634, 2006.*

[10] Aleecia M. McDonald. Cookie confusion: do browser interfaces undermine understanding? In *CHI EA '10: Proceedings of the 28th of the international conference extended abstracts on Human factors in computing systems*, pages 4393–4398, New York, NY, USA, 2010. ACM.

[11] Aleecia M. McDonald and Lorrie Faith Cranor. Americans' attitudes about internet behavioral advertising practices. In *WPES '10: Proceedings of the 9th annual ACM workshop on Privacy in the electronic society*, pages 63–72, New York, NY, USA, 2010. ACM.

[12] Microsoft. Oh My God, I'm Gonna Puke, 2009. `www.youtube.com/watch?v=xB9fhjnJcB0`.

[13] Microsoft. 8 Second Demos – Private Browsing, 2010. `www.tellyads.com/show_movie.php?filename=TA10531`.

[14] Microsoft. Internet Explorer 8: Features, 2010. `www.microsoft.com/windows/internet-explorer/features/safer.aspx`.

[15] Joshua Sunshine, Serge Egelman, Hazim Almuhimedi, Neha Atri, and Lorrie Faith Cranor. Crying wolf: an empirical study of ssl warning effectiveness. In *SSYM'09: Proceedings of the 18th conference on USENIX security symposium*, pages 399–416, Berkeley, CA, USA, 2009. USENIX Association.

[16] Joseph Turow, Jennifer King, Chris J. Hoofnagle, Amy Bleakley, and Michael Hennessy. Americans Reject Tailored Advertising and Three Activities that Enable It. *SSRN eLibrary*, 2009.

[17] Hamilton Ulmer. Understanding Private Browsing. *Blog of Metrics*, August 23 2010. `blog.mozilla.com/metrics/2010/08/23/understanding-private-browsingl`.

[18] Nick Wingfield. Microsoft quashed effort to boost online privacy. *The Wall Street Journal*, August 2 2010. `online.wsj.com/article/SB10001424052748703467304575383530439838568.html`.