An Analysis of the 'Do Not Track' Header

By Ben Goodrich

Abstract

The proposed 'Do Not Track' HTTP header is a bit flag passed by the client to a webserver that indicates the user's preference for being tracked by advertising agencies through the use of cookies. The user can choose to 'opt out' which means they don't want to be tracked, 'opt in' which means they do want to be tracked, or 'none specified' which means that they simply didn't provide a value. Currently, each of the major web browsers except for Google Chrome supports the DNT header, but since there is no law regarding compliance with the header's specification, most advertising agencies do not honor the header and will track the user regardless of their preference. There have been several proposals in congress to create laws to enforce the statutes of the Do Not Track header, however none of them have made it into a law. This paper examines the history of the Do Not Track header, the current state of the world regarding compliance, and the feasibility and outcomes of mandating compliance with the header.

Introduction

What The Do Not Track Header Is

The 'Do Not Track' header (henceforth known as the DNT header) represents a backlash against the continual erosion of privacy in the modern world and especially on the internet for average users. Advertising agencies have begun tagging visitors to specific websites with cookies, which can then be used to uniquely identify and track that user as they continue to browse the internet, well after they have left the site that had the advertiser's content. This information can then be exploited by the advertiser to target the user with ads based on the information that the advertiser has gained about the user's browsing history. For example, if a user is found to be visiting a large number of jewelry websites, the ad network could then target that user with advertisements for other jewelry sites that have paid for advertising with them. While this doesn't seem like a huge imposition on the surface, it really does end up being an invasion of an individual's privacy and could lead to a wide variety of unforeseen problems. For example, if that tracking data were to be stolen from the advertiser, it could potentially be used to blackmail or embarrass the people whom the information pertains to. The DNT header represents a way for users to control how the information being gathered about them is used by advertisers and corporations. It's simply a flag that tells advertising agencies whether the user wishes to be tracked and targeted with ads or whether they'd rather opt out and maintain their privacy.

How The Header Works

The DNT header is a bit flag optionally included in the HTTP header of an HTTP message. The purpose of the flag is to indicate to the server receiving the request whether they are permitted to track the user's browsing habits in order to serve them with targeted advertising. If the flag is set to a value of '1' it means the user wishes to opt-out of tracking. In

other words, the advertisers should not be tracking them and targeting them with ads. If the flag is set to '0' it means that the user wishes to opt-in and does not mind if advertising agencies track them and target them with advertisements. The final option is omitting the flag entirely, which means the user has not expressed a preference. (Mayer)

To the community

Today's society has seen an unprecedented and drastic reduction in privacy for individuals. From Facebook, Twitter, and other social networking sites to increased ease of monitoring by government and state agencies, the average person has both willingly and unwillingly given up a large portion of their privacy over the last twenty years. So, it becomes increasingly important to maintain any scraps of privacy left, at least for the people who wish to have some privacy. Through regulation, awareness, and anonymizing technologies some of that privacy can be retained. This paper is devoted to highlighting a very specific, but rather important example of a piece of technology (coupled with awareness and potentially legislation) that can help protect privacy for an average internet user.

History of the Do Not Track header

Summary of the History of the DNT Header

The roots of the DNT header began in 2007 after the success of the 'Do Not Call' list for phones. Hoping to emulate the success of the DNC list, several groups such as the EFF and World Privacy Forum attempted to persuade the FTC to create a similar 'Do Not Track' list for online advertising. (Soghoian) It would have required advertisers to register information with the FTC so that information could then be used by browser plugins (or the browser itself) to block tracking. Unfortunately, it didn't catch on, and the concepts behind 'Do Not Track' were pushed to the back burner for a couple years.

Then, in 2010 the chairman of the FTC, Jon Leibowitz, resurrected the idea of a way for individuals to opt out of tracking by advertising agencies. In front of the senate, during an 'online privacy' hearing, he again suggested the possibility of a 'Do Not Track' list. (Soghoian)

Throughout all this time, there was a push from a technological perspective to allow users to block advertisers from tracking them. For quite a while, online advertisers had been offering individuals the ability to opt out of being tracked by their network by keeping a cookie in their browser that indicated they didn't want to be tracked. Unfortunately, these cookies suffered from two problems. The first was that they only worked for a single advertising network. The second was that if the user cleared their cookies, the DNT cookie would be wiped out with them, and the individual would have to re-obtain the DNT cookie from the advertising network. This led Google to create a browser add-on that allowed users to manage their cookies in such a way that it wouldn't wipe out the cookie used to opt-out of Google's own advertising network, doubleclick.net. (Soghoian) From there, a browser add-on named Targeted Advertising Cookie Opt-out (TACO) was developed for Firefox. TACO was continually updated to include new advertising networks so that users could opt-out of a large portion of them at once. The developers of TACO and the Mozilla Foundation soon realized that maintaining a list of advertising network opt-out cookies would be unmanageable in the long term and so talks about an HTTP header which indicated whether a user wished to be tracked started to spring up. (Soghoian) From these talks, arose the concept of the DNT header as it is known today.

Other Options for Privacy for an Average User

There exist other options for individuals who wish to remain anonymous to advertising networks. These include using anonymizing proxies and 'private browsing' modes in browsers. Each of these provides some solutions but also has problems. Proxies tend to slow down your internet connection substantially and whoever controls the proxy can see any traffic going across it, so the owner of the proxy has to be trusted. Additionally, having a proxy doesn't prevent cookies from being stored on your machine and so even if the advertising network can't identify you directly, they can still track your browsing habits. Private browsing modes don't slow down your connection and they also don't prevent cookies from being stored on your computer. They do, however, delete all of the browser cookies when you close the private browsing session, which can help to prevent tracking between sessions of internet use. However, they can't delete all of the cookies on your machine, such as flash cookies, so they cannot be guaranteed to defend against all tracking. (Conley)

Current State of the world regarding compliance

Technology

Currently each of the major browsers (Internet Explorer, Firefox, and Safari) except Google Chrome supports allowing the user to opt-out of tracking by using the DNT header. Google plans to add this functionality to Chrome soon. (Mark) Google's claimed reasons for slow adoption of the DNT header are that the definition of 'Do Not Track' is very ambiguous, there is little adoption by the advertising networks, and that they already have a plugin which allows a user to keep their opt-out cookies between wipes of cookie storage. (Singel)

Very few, if any, advertising networks currently honor the DNT header. An analysis done by pcmag.com showed that neither google's ad network nor doubleclick ad network honored the DNT header. With the header turned on, the writer of the article was still getting cookies from both networks stored on his computer. However, when using IE9 with a block list, both of these networks were prevented from storing tracking cookies on the writer's computer. (Muchmore) Unfortunately, IE9's block list is similar to TACO in that it is simply a list of networks whose cookies are blocked by the browser as opposed. Its success is not evidence that those networks are honoring the user's wishes.

Laws

There are currently two laws in congress regarding a user's ability to opt out of being tracked. However, both of the laws are stalled. The FCC chairman has stated in a report that a law regulating advertiser's use of tracking cookies may not be required, given the progress many advertising networks have made recently regarding starting to work on honoring DNT headers. However, according to an analysis by pcworld.com, if there isn't enough progress by those networks soon, there will be more pressure to pass laws regulating tracking individuals on the internet. (Gross)

Possible outcomes of DNT header regulation

There are many possible positive and negative outcomes from enacting laws regulating tracking of individuals and compliance with DNT header preferences, however it seems that in general the net effect would be a positive result. The negative effects would mostly be for the

advertisers. They wouldn't be able to target advertisements as well and they would have to spend more money targeting groups in other ways. The positive results would be increased privacy for individuals who opt-out, increased individual control over how their data is used, and increased trust of advertising networks. Additionally, if there was regulation regarding use of personal information for corporations, there could be punishments for those companies that broke the rules and exploited private information. Individuals would have recourse to reclaim some of the cost of having personal information leak to malicious hands. The issue with regulation, however, is that the internet is an international entity and any laws enacted in the United States would only apply to companies that had a presence here. If companies outside the United States (and perhaps friendly nations) decided to break the rules regarding the DNT header and private information, there would be little recourse for individuals targeted by those corporations. This imbalance in regulation could provide a strong competitive edge for advertising companies based outside of the United States and could drive some of the U.S.'s larger advertising agencies out of the country or out of business.

Action Items

Below are instructions on how to turn on the DNT header in various browsers that support it.

Turning on DNT in Firefox On Linux

Edit->Preferences->Privacy and click 'Tell websites I do not want to be tracked'

Turning on DNT in Firefox on Windows

Tools->Options->Privacy and click 'Tell websites I do not want to be tracked'

Turning on DNT in Internet Explorer 9

Navigate to http://ie.microsoft.com/testdrive/Browser/DoNotTrack/Default.html. Click on the link with the text 'Click here to add an empty Tracking Protection list. Click the 'Add List' button.

In addition to activating the DNT header in their browser, people can encourage companies to honor the header by writing to their congressman or congresswoman in support of regulation enforcing the meaning of the header.

Conclusion

In a world where privacy is constantly eroded through the actions of corporations and because of individual willingness to freely give out personal information, it becomes increasingly important to allow individuals to decide how, when, and in what capacity their personal information is used. Technology like the 'Do Not Track' header is a first stepping stone towards giving people control over their own data. The perils of a society that places no value on a person's right to privacy are plentiful and apparent and so as the internet continues to become a central focus of people's daily lives, it is important to build tools to accompany it that allow individuals to decide how private they wish their lives to be. It will be necessary to enact rules and regulations regarding the use of private personal information as well, because if there are no rules then punishment for misuse of that information becomes nearly impossible and people will have no recourse if they are harmed by such misuse.

Works Cited

Conley, Chris. aclunc.org. How Private is Private Browsing. American Civil Liberties

Union, 29 Dec. 2008. Web. 1 May 2012. http://www.aclunc.org/issues/technology/blog/how_private_is_private_browsing.shtml

Gross, Grant. *PCWorld*. FTC Chairman: Do-Not-Track Law May Not Be Needed. IDG News, 26 Mar. 2012. Web. 30 Apr. 2012. http://www.pcworld.com/businesscenter/article/252556/ftc_chairman_donottrack_law_may_not_be_needed.html>

Mark, Gary. *BrowserFame*. Google and Chrome to Support 'Do Not Track'. n.p., 23 Feb. 2012. Web. 30 Apr. 2012. http://browserfame.com/478/google-chrome-support-do-not-track

Mayer, Jonathan. and Arvind Narayanan. *DoNotTrack.us.* Do Not Track - Universal Web Tracking Opt Out. Stanford, n.d. Web. 30 Apr. 2012. http://donottrack.us/>

Muchmore, Michael. *PCMag.* The State of 'Do Not Track' in Current Browsers. n.p, 27 Mar. 2012. Web. 1 May 2012. http://www.pcmag.com/article2/0,2817,2402168,00.asp

Singel, Ryan. *Wired.* Google Holds Out Against 'Do Not Track' Flag. n.p., 15 Apr. 2011. Web. 30 Apr. 2012. http://www.wired.com/epicenter/2011/04/chrome-do-not-track/ Soghoian, Christopher. *Slight Paranoia.* The History of the Do Not Track Header. n.p, 21 Jan. 2011. Web. 1 May 2012. http://paranoia.dubfire.net/2011/01/history-of-do-not-track-header.html