Network Working Group	A. Cooper
Internet-Draft	Center for Democracy & Technology
Intended status: Informational	H. Tschofenig
Expires: May 28, 2012	Nokia Siemens Networks
	November 25, 2011

Overview of Universal Opt-Out Mechanisms for Web Tracking
draft-cooper-web-tracking-opt-outs-00

Abstract

Web servers and the entities that operate them have long had the ability to track user agents as they access resources hosted across different web domains. Concern over the privacy implications of such tracking has prompted recent work on a number of solutions that aim to provide a universal opt-out mechanism for web tracking that can be effectuated through a simple binary choice presented to users.

This document provides an overview of the following mechanisms: permanent opt-out cookies, cookie blocking, domain blocking, a "Do Not Track" (DNT) HTTP header, and a Do Not Track Document Object Model (DOM) property. The aim of this document is to describe each approach, the pros and cons of each, and areas where standardization may be necessary should each approach be further pursued, without making recommendations about which approach or approaches should be adopted.

Status of this Memo

Copyright Notice

as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction

The Hypertext Transfer Protocol (HTTP) is a generic and stateless application-level protocol for distributed collaborative hypermedia information systems. The stateless nature of the HTTP protocol is a useful property for scalability and for robustness. However, for more complex web sites it is often important to carry state information between different web pages and to offer reidentification of previous visitors for usability reasons. This has lead web application developers to invent mechanisms for maintaining state information about end user interactions. In fact, one mechanism - the cookie (originally specified in [RFC2109] and now being revised by [I-D.ietf-httpstate-cookie]) - has been added to HTTP itself. Since cookies come with limitations, such as the number of cookies that are allowed to be stored per domain, the size of an individual cookie, and the total number of cookies that can be stored, it is not the only state management concept used by developers. Other mechanisms include combinations of server-side databases, hidden form fields, URL query parameters, extensions to the CGI model, storage capabilities offered by additional plug-ins (such as Adobe Flash and

Microsoft Silverlight), HTML5 web storage, and special browser extensions (such as Internet Explorer's userdata behavior).

State created by the web server allows the server to uniquely identify individual user agents, providing a mechanism to correlate information about the activity of a single user agent across requests for different resources. Many of today's web sites cause user agents to fetch resources from a large number of other sites which may also make use of state management techniques.

State information, such as cookie state stored within the browser, is not accessible to every site due to user agent security policies (which may include the same-origin policy [I-D.abarth-principles-of-origin] and its variations), but sharing of information between web sites visited by a single user can take many different forms. Data may be shared between two sites that both cause requests to the same third site, by sites that share DNS CNAME records or authoritative DNS servers, or between sites that share identifying URLs or referer headers [Krishnamurthy06] [Krishnamurthy07]. These techniques, together with uses of cookies, Javascript, Flash, and other mechanisms for data aggregation purposes, have become pervasive among popular web sites [Krishnamurthy09], allowing users to be tracked in a multitude of ways.

Concern over the privacy implications of this tracking has prompted recent work on a number of different solutions that aim to provide a universal opt-out mechanism for web tracking that can be effectuated through a simple binary choice presented to users. This document provides an overview of several such mechanisms.

1.1. History of Opt-Out Cookies

Web tracking was first widely employed by "third-party" advertising networks, which locate their advertising resources at their own domains (not at the "first-party" domains to which user agents typically issue requests at the direction of users). User agent requests for top-level documents from many separate first-party domains often generate requests for resources that are all located at the same third-party ad network domain, providing the ad network with the ability to build a profile of the first-party resources accessed by the user agent. Ad networks then use these profiles to individually tailor ads served to a particular user agent. This practice is known as "behavioral advertising."

Concern over the privacy implications of the tracking involved in behavioral advertising gave rise in 1999 to the Network Advertising Initiative (NAI), a consortium of online advertising companies [NAI-History]. Shortly after its formation, the NAI developed a set of guidelines that its member companies were bound to follow. Among these guidelines was a requirement that the ad companies provide web users with the ability to opt out of ad targeting [NAI-Guidelines].

The primary mechanism adopted for effectuating the opt out was an "opt-out cookie": an HTTP cookie that stores the user's preference to be opted out of ad targeting. Under the guidelines, NAI members could provide users with links to set their opt-out cookies from their own web sites and from a central site [NAI-Registry]. A newer central

site now provides users with access to the opt-out cookies for companies that are members of a number of other advertising trade associations in addition to the NAI, all of which are operating under the banner of the Digital Advertising Alliance (DAA) [DAA10].

1.2. Drawbacks of Opt-Out Cookies

Several drawbacks to the opt-out cookie approach have been identified over time. Storing the user's preference in a cookie is problematic because users are often encouraged to delete their cookies in order to protect their privacy. If they follow this advice, they delete their opt-out cookies as well, and ad targeting resumes.

Because HTTP cookies are typically only returned to the origin server that set them [I-D.ietf-httpstate-cookie], using cookies to control user preferences requires that users obtain individual opt-out cookies for each tracking domain. With current upper estimates for the number of tracking domains reaching over 300 [PrivacyChoice-Tracker-Index], this creates a complex cookie management task for users.

Not all of these tracking domains are used for behavioral advertising. Tracking -- in the generic sense of correlating a single user agent's requests across multiple domains -- is used for a number of other purposes, including web analytics, web site personalization, ad reporting (e.g., calculating the number of ad views or clicks), market research, fraud detection, and federated authentication. Like behavioral advertising, some of these services (web analytics, ad reporting, some market research services) use cookies as their primary means of identifying user agents and could therefore make use of opt-out cookies to store user preferences. But recent investigations have indicated that only about half of the 300 or so tracking domains offer opt-out cookies [Brock11]. Meanwhile, the DAA site offers the opt-out cookies of only about 60 companies.

For some of the other tracking purposes, using an opt-out cookie would make little sense. For example, a site or service that requires users to authenticate to obtain access to a personal profile might find it more reasonable to store the user's opt-out choice on a back-end system as part of the user's profile. Since cookies were designed to overcome the statelessness of web transactions, any site or service that persists state about individual users in some non-cookie-based storage can likely find a more streamlined way to store individual opt-out preferences than by using opt-out cookies.

Opt-out cookies also do not control tracking that makes use of other technologies. Flash cookies, HTML5 web storage, browser fingerprinting, the CSS history leak, and a number of other non-HTTP-cookie mechanisms can be used to track web activity across domains [Kamkar10][EFF][Baron10].

1.3. New Tracking Opt-Out Mechanisms

For all of these reasons, a number of new solutions have been proposed to improve upon the status quo for opting out of web tracking. While these mechanisms differ in their implementations, they share a similar goal: to provide a universal opt-out for web

tracking that can be effectuated through a simple binary choice presented to users (this will be referred to hereafter as the "DNT goal"). This document provides an overview of the following mechanisms:

2. Terminology: First Party vs. Third Party

There are a number of web-related terms that have taken on special meaning within discussions about web tracking. Some of these meanings may differ from the common understanding of the same terms in the IETF context.

In the context of web tracking, a "domain" usually refers to the portion of a web resource's host name comprised of the second-level domain and top-level domain. For example, the domain corresponding to http://count.example.com/ would be example.com. The term "subdomain" is often used to describe a fully qualified domain name (FQDN). For example, the URI http://count.example.com/ contains the subdomain count.example.com.

A "first-party domain" usually refers to the domain of a web site to which a user agent directs an explicit request on behalf of a user. A "third-party domain" usually refers to the domain of a web resource that a user agent requests as a result of a first-party request. A third-party resource is hosted at a different domain from the first-party domain that triggers the third-party request. As an example, if a user directs his user agent to http://www.foo.com/ and as a result the user agent also makes a request to www.bar.com, foo.com is the first-party domain and bar.com is the third-party domain.

This distinction between first-party and third-party domains is in part a result of long-standing user agent practices for handling HTTP cookies. Typically, HTTP cookies are returned only to the origin server that set them [I-D.ietf-httpstate-cookie]. Cookies set from first-party domains may not be read by third-party domains and vice versa. In some cases, cookies set from first-party domains that contain subdomains are accessible by all subdomains of the first-party domain. The distinction between first-party domains and third-party domains is reflected in browser-based cookie controls: major web browsers all offer distinct first-party cookie settings and third-party cookie settings.

However, a user's perception or expectation of the difference between a "first party" and a "third party" may not fall neatly within the distinction between "first-party domain" and "third-party domain." Consider Example Company, which hosts its web site at example.com and contracts with an analytics service provider, Count Company. The analytics service is architected such that it operates from count.example.com, a subdomain. When a user visits www.example.com, a request is triggered to count.example.com, and data about the user's visit is returned to count.example.com to be processed by Count Company. Although all of these exchanges would be between the user agent and first-party domains, the user may only expect to be sending data to Example Company (the "first party"), not to Count Company (the "third party").

Conversely, consider that Example Company runs a social network, Example Social, hosted at examplesocial.com, and a photo-sharing service, Example Photos, hosted at examplephotos.com. Example Social might have a feature that allows users to share their photos from Example Photo on their profiles hosted at examplesocial.com. In this case, a user agent that requests a resource hosted at examplesocial.com would also automatically request and receive content hosted at examplephotos.com. While user agents might consider examplephotos.com to be a third-party domain, the user might consider all the content they receive to be coming from a single first party, Example Company.

It has been suggested that this distinction between first parties and third parties from the user expectation perspective can be approximated by distinguishing domains based on their Public Suffixes [Mozilla] plus one additional domain label ("PS+1") [I-D.mayer-do-not-track].

In the remainder of this document, "first-party domain" and "third-party domain" will be used to describe the typical distinction used by web browsers between the two types of cookies; the terms "first party" and "third party" will be used when the user expectation perspective is more appropriate.

A summary of the terminology used in the document (some of which is drawn from [I-D.mayer-do-not-track]) is as follows:

*Domain: The portion of a web resource's host name comprised of the second-level domain and top-level domain.

*DNT goal: To provide a universal opt-out for web tracking that can be effectuated through a simple binary choice presented to users.

*First party: A functional entity with which a user reasonably expects to exchange data.

*First-party domain: The domain of a web site to which a user agent directs an explicit request on behalf of a user.

*Third party: A functional entity that a user does not reasonably expect to receive the user's data.

*Third-party domain: The domain of a web resource that a user agent requests as a result of a first-party request.

3. Tracking Opt-Out Mechanisms

The mechanisms described in this section are at various stages of development, deployment, and standardization. The mechanisms are not necessarily mutually exclusive; it is possible that a combination of approaches could be employed to fulfill different aspects of opt-out functionality, although the mechanics of such combinations are out of scope for this document. It is also possible that some of the mechanisms or similar concepts could be adapted to address tracking outside of the web context -- for example, within mobile applications or email applications. These other contexts are likewise out of scope.

Much of the privacy concern about web tracking has focused on tracking conducted by third parties because it often occurs without the knowledge of users and is performed by companies with which users may have no relationship. However, tracking may also be performed by first parties. For example, first parties may track users in order to provide personalized or customized content, or they may share information about user agent requests with third parties who then aggregate that information across multiple first parties. While the traditional opt-out cookie approach does not address first-party tracking, some of the newer mechanisms could be implemented in a way so as to address first-party tracking. A discussion of the extent to which each of the mechanisms addresses first-party tracking is included in the sections below.

3.1. Permanent Opt-Out Cookies

A number of web browser extentions exist to make opt-out cookies permanent: Targeted Advertising Cookie Opt-Out (TACO) for Firefox and Google Chrome [Abine11], Keep My Opt-Outs (KMOO) for Chrome [Google11], and Keep MORE Opt-Outs, developed by PrivacyChoice [PrivacyChoice11]. These extensions first install the opt-out cookies for a number of ad companies -- all NAI members for KMOO and larger lists of companies for the other two extensions. If the user already has uniquely identifying cookies for any domains on the list, those cookies are deleted. Thereafter, the extensions wait for a cookie change event and preserve the opt-out cookies even when a user clears his or her cookies.

The main benefit of this approach is that it does not require any changes on the server side. Servers used to track user agents can continue to operate as they have since opt-out cookies were first introduced. This approach can also apply to tracking conducted for many different purposes or to tracking from first-party domains -- any domain that offers an opt-out cookie could be included in the list of domains for which the browser extension installs an opt-out cookie. Keep MORE Opt-Outs, for example, takes this approach.

While this approach overcomes one of the limitations of opt-out cookies -- their lack of persistence -- it still requires managing potentially hundreds of opt-out cookies and ensuring that the list of precisely which opt-out cookies to retain remains up-to-date even as entities that track reconfigure their own cookie-setting practices on the server side. This may amount to a complex managerial task for the browser extension developer. Furthermore, for all entities that conduct tracking but do not offer an opt-out cookie -- of which there are potentially hundreds -- this approach will not work for those entities' domains.

Most opt-out cookies do not contain unique user agent identifiers, so installing a domain's opt-out cookie and deleting other uniquely identifying cookies from that domain will generally prevent that domain from continuing to track the user agent via HTTP cookies (while also providing a way for users to verify that they have been opted out). However, in general it does not prevent tracking via other means such as Flash cookies or HTML5 web storage.

No existing implementations of this approach exist natively in user agents; they are all currently browser extensions that require user-initiated installation. If this approach were to be pursued further, there may be a need to specify a standard way of representing the list of opt-out cookies that a particular user agent or extension makes permanent and/or the rules for processing the list (similar to what may be required to standardize block lists, see Section 3.3).

3.2. Cookie Blocking

Since much web tracking has historically occurred via HTTP cookies, it has been suggested that providing users with simple settings to turn cookie blocking on and off may serve the purpose of a universal, binary tracking opt-out choice. All of the major web browsers offer blanket settings for blocking all third-party cookies. However, current implementations differ in their functionality; for example, in some browsers, blocking third-party cookies prevents third-party cookies that the user had previously downloaded from being read, whereas in other cases pre-existing third-party cookies can continue to be read and the block merely prevents new third-party cookies from being set on a going-forward basis. This kind of variation reflects different evaluations of the trade-off between the benefits of more comprehensive blocking and the potential for cookie blocking to alter or break the functionality of certain web sites.

The main advantages of the cookie-blocking approach are that it targets what is still the most common means of tracking (HTTP cookies) and it is already built into the most widely used web browsers. However, because of the variations across the browsers, some implementations -- particularly those that continue to allow some third-party cookie reading or setting even after users have affirmatively chosen to block third-party cookies -- may not match users' expectations of what a universal tracking opt-out solution should accomplish.

On the other hand, complete third-party cookie blocking does have the potential to inhibit the functionality of some web sites (including functionality unrelated to tracking). Some sites may even prevent users from accessing the sites unless they re-enable third-party cookies. This kind of behavior serves as a disincentive to using existing cookie-blocking settings as a means to achieve the DNT goal.

When it prevents uniquely identifying third-party cookies from being read, cookie blocking can be an effective and user-verifiable tool for opting users out of tracking of all kinds. In addition to third-party cookie blocking, most browsers also provide a setting to block all first-party cookies, but because use of this setting breaks significant amounts of web functionality, it is not a reasonable mechanism for opting out of tracking from first-party domains. Nor does cookie blocking have any effect on tracking that occurs via other means.

3.3. Domain Blocking

Domain blocking requires the user agent to maintain a list of domains to block and to block requests that the user agent would otherwise make to domains on the list. If the list is comprised of domains from

which tracking occurs, domain blocking prevents tracking by preventing the user agent from communicating with those domains. Domain blocking has been used for years to block web content of many different kinds, including advertising (see, for example, the AdBlock Plus extension for Firefox and Chrome [AdBlock-Plus]). The Tracking Protection feature in Microsoft Internet Explorer 9 makes use of third-party domain blocking (among other functionality) [Microsoft10]. Many implementations of domain blocking have the ability to periodically update their block lists (by contacting some authoritative source) to stay up-to-date with server reconfigurations and other changes.

Although giving users a simple binary choice about blocking a list of domains is likely sufficient to achieve the DNT goal, the domain blocking approach can also include more granular options that give users finer-grained control over their web communications. Existing implementations allow blocking at the level of a subdomain, path or file, for example. They also combine domain blocking with domain whitelisting so that certain domains are kept affirmatively reachable.

Domain blocking is a powerful solution because it entirely prevents tracking from occuring via any mechanism that originates with a web server request, including cookie setting, other HTTP-header-based mechanisms, and the transmission of scripts, images or other files that trigger tracking. Domain blocking is also verifiable in that observing requests issued by the user agent will demonstrate that domains on the list are not being accessed.

However, to an even greater extent than cookie blocking, domain blocking may cause site functionality to break. For domains that conduct tracking and serve content from the same domain, blocking will prevent both the tracking and the content delivery, even if the user desires to opt out of the tracking without losing access to the content or some version of the content. Domain operators that want to be able to continue serving content and tracking user agents in the face of pervasive domain blocking would need to conduct these activities from separate domains (as was envisioned in the original proposal for behavioral advertising domain blocking [CDT07]), keeping only the tracking domain on the block lists. In some cases this change could require significant costs in terms of server reconfiguration. Moreover, domain operators whose domains are placed on block lists against their will could seek to avoid being blocked by switching domains (possibly on a recurring basis to circumvent list updates). And as with cookie blocking, first-party domains that detect domain blocking may require users to turn domain blocking off before providing access to first-party content.

Domain blocking requires that the list of domains to block be kept up-to-date, which may require some management overhead. Domain blocking cannot be used to block first-party tracking since blocking first-party domain requests would prevent users from accessing content that they explicitly wished to access.

The IE 9 Tracking Protection feature allows for block lists to be independently created according to a specified file format. The format and the rules for processing block list entries have been

submitted to the W3C for potential standardization [Zeigler11]. AdBlock Plus has its own filter list format [AdBlock-Plus-Filters]. Ultimately, standardization of the block list format and processing rules is likely to be required if the goal is for multiple user agents to be able to use the same independently created block lists.

3.4. Do Not Track HTTP Header

The proposed Do Not Track HTTP header is a user agent feature that appends a new header to HTTP requests that expresses the user's preference not to be tracked. In existing header implementations, the header value is binary: 1 means no tracking and 0 means tracking is permissible. Users can control whether the header is sent through a simple browser preference. A DNT header has been implemented in the current Firefox beta [Stamm] and in a number of browser extensions [Soghoian][Palant11][NoScript]. Depending on the user agent's policy, the header could be appended to every web request, or to a subset of requests (for example, only third-party domain requests, or all requests aside from those for which the user has explicitly chosen to permit tracking).

Unlike the mechanisms already discussed, the DNT header does not provide a technical means of enforcing any sort of ban on tracking. Cookies and other tracking mechanisms would still be operational. Thus the presence of the header does not run the risk of directly interfering with existing web site functionality (as cookie or domain blocking might).

Rather, the header provides a statement of the user's preference to the domains to which the user agent makes requests. This creates the possibility for the header to provide much broader-based protection against tracking than the other mechanisms if the majority of tracking entities abide by it. Every tracking entity that receives the header would be able to act on it, including first parties, entities that use tracking for purposes other than behavioral advertising, and entities that track users via mechanisms other than HTTP cookies.

The lack of a technical enforcement mechanism creates a need to develop some common understanding of what "tracking" means, how domain operators should behave when they receive the header, and to whom the header applies. Should first parties that share tracking data with third parties be required to abide by the header? Should first parties and third parties be distinguished by domain name or by user expectation? Should tracking for certain purposes (fraud detection or ad reporting, for example) be permitted regardless of whether the header is present? Should the header affect the extent to which web request data is retained on the server side? There are a number of efforts underway to try to develop some consensus about the answers to these and other questions in a way that balances the realities of web server operation, legitimate uses of web request data, and users' desire for privacy protection [Mayer][CDT11] [Eckersley11]. One of these efforts is seeking to define the semantics and intended usage of the header in the context of its potential standardization at the IETF [I-D.mayer-do-not-track]. How these questions are answered will determine the extent to which

server-side reconfiguration is necessary for entities that wish to honor the header.

Until some sort of consensus is reached about the semantics and usage of the header on the server side, the level of protection against tracking that the header affords will remain uncertain. Even if a common semantic were established, the header would still require users to trust that their web request data, including unique identifiers sent via cookies or other means, would not be used for tracking whenever the header is present. This sort of guarantee may require enforcement or intervention from governmental privacy authorities in order to truly be effective.

As with cookie blocking, some sites that detect the header may prevent users from accessing their content, or they may request that users turn the header off before access is granted. If the header is deployed without granular user control over the sites to which it is sent, this kind of server-side reaction to the header could incentivize users to simply turn the header off entirely, because they would have no way to send the header to some sites but not others. Regardless of whether controls exist or not, having individual sites that ignore the header or that ask users to disable it frustrates the DNT goal of having a universal, binary opt-out mechanism.

For a DNT header to be interoperable across web sites and user agents, it would need to be defined according to the syntax specified in the HTTP protocol specification [RFC2616] and registered according to the procedures in RFC 3864 [RFC3864]. This path is currently being pursued in [I-D.mayer-do-not-track]. Standardization of the header has also been proposed to the W3C [Zeigler11].

3.5. Do Not Track DOM Property

In a similar vein to the DNT header, the Document Object Model (DOM) could be extended to include a property that expresses the user's preference with respect to tracking. Users could set the value of the property through a simple browser preference, causing the property to be set for all documents (or for documents from some subset of domains, with exceptions specified by the user). Client-side code could query the property before taking tracking-related actions.

The DOM property has similar advantages and disadvantages as the header. Its mere deployment need not interfere with any existing web functionality. It has the potential to be accessed and respected by first parties and trackers of all kinds, although its applicability is limited to sites architected to have access to the DOM -- tracking that occurs entirely on the server side will be unaffected by the property. Responding to the presence of the property will require some shared understanding of the property's semantics. Its presence may lead sites to request that users allow tracking in order to access the desired content.

One way in which the property differs from the header is that it may reduce the number of server calls made on behalf of users who opt out of tracking. This could be the case if detection of the property causes client-side code not to make requests to tracking domains that

otherwise would have been made. This lack of requests issued on behalf of users who have opted out could provide a limited means for users to verify that their preference is being honored -- if users who set the property to the "no tracking" setting observe fewer or different server calls than users who allow tracking, this may provide some proof that sites are honoring the property, although this would likely need to be evaluated on a site-by-site basis since sites may need to implement their responses to the property differently.

As with the header, for the DOM property to be interoperable, its syntax and semantics would need to be standardized. A DNT DOM property has been proposed to the W3C for standardization [Zeigler11]

4. Security Considerations

This document describes various mechanisms that allow users to opt-out of web tracking. Thus one way to frame the security goal of these solutions is the prevention of information leakage to those doing the tracking, particularly third parties. The adversary from a user agent point of view can therefore be considered to be any third party that conducts tracking.

Because any information that is shared with a third party could potentially be used to identify a user agent, altogether preventing communication with third-party domains when a user contacts a first-party domain is perhaps the most intuitive way to prevent information leakage to third parties. For example, a user agent might be configured to serve content only from example.com when a user enters http://www.example.com in the browser address bar. However, this approach of preventing all third-party communications is unrealistic since today's web sites often combine content aggregated from many other sites. Hence the task of preventing third-party tracking is more complicated. To address this complexity, the mechanisms discussed in this draft are either more subtle or more granular (or both) than all-out blocking of third parties, and they all face a number of security challenges.

Regardless of whether any opt-out mechanism is used, first parties always have the ability to convey information related to tracking to third parties through an out-of-band or back-end channel. Since user agents cannot observe these exchanges, there is little they can do to prevent them.

The same origin policy treats subdomains as belonging to the first-party domain. However, a first party can configure its DNS servers in a way that a DNS CNAME alias points to a server belonging to another organization. With appropriate cookie settings by the first party, it is possible for the third party to obtain access to all cookies. Permanent opt-out cookies, cookie blocking, and domain blocking are not able to prevent this data sharing if they are configured to respect the usual same origin policy. A DNT header or DOM property may prevent this sharing if the first party respects the user's preference as signaled by the header or property.

All techniques that block direct communication to specific third party sites (via a block list mechanism) suffer from the generic

limitations of blacklisting mechanisms. Third parties that want to avoid being blocked will regularly change their domains, attempt to require users to exert additional effort in order to manage blacklists, or relay communication through intermediaries to obfuscate the identification of their domains. To emphasize the negative impact on user experiences that blacklisting can have, some third parties may bundle extra functionality onto the same (blocked) domain, rendering it inaccessible to those using block lists.

The online management of block lists raises questions about who provides the lists, how easy they are for users to download or reconfigure, which list is used by default, what security mechanisms control the manipulation of the lists, and what conflict resolution mechanism is offered when black and white lists are combined. The answers to these questions depend heavily on the technology chosen for managing the lists. Failing to secure the lists against manipulation could allow information to be leaked to third parties against the user's wishes.

Mechanisms that convey user preferences in a header or as a DOM property will require the receiving party to adhere to the instructions. As with the block listing mechanisms, implementation details pertaining to the default settings in browsers, the ease of changing the settings, and whether the settings can be manipulated will affect the security of the settings themselves.

Some web proxies, gateways, and other intermediaries are known to strip certain HTTP headers (the Referer header, for example) or only allow a strict set of HTTP headers to pass through. While third-party companies are unlikely to have the incentive to cooperate with these intermediaries for the explicit purpose of removing or modifying the DNT header, such removal would result in the user's preference not being expressed to receiving servers. Scripts could be used to modify or disable the DNT header or DOM property within the browser to achieve the same effect, but these are fairly easy to detect and therefore unlikely to be abused by third parties that want to conduct tracking against the user's will. Given that third parties can simply ignore the user's preference if they want to conduct tracking under the DNT header or DOM property scenarios, these attacks are unlikely to be used.

5. IANA Considerations

This document makes no requests of IANA.

6. Acknowledgments

The authors would like to thank Michael Hanson for inspiring the work on this draft and Justin Brookman, Sue Glueck, and Erica Newland for their reviews.

7. References

[I-D.ietf-httpstate-cookie]	Barth, A, "HTTP State Management Mechanism", Internet-Draft draft-ietf-httpstate-cookie-23, March 2011.

[I-D.abarth-principles-of-origin]	Barth, A, "Principles of the Same-Origin Policy", Internet-Draft draft-abarth-principles-of-origin-00, February 2011.
[I-D.mayer-do-not-track]	Mayer, J., Narayanan, A. and S. Stamm, "Do Not Track: A Universal Third-Party Web Tracking Opt Out, draft-mayer-do-not-track-00 (work in progress)", March 2011.
[RFC2616]	Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P. and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.
[RFC3864]	Klyne, G., Nottingham, M. and J. Mogul, "Registration Procedures for Message Header Fields", BCP 90, RFC 3864, September 2004.
[RFC2109]	Kristol, D.M. and L. Montulli, "HTTP State Management Mechanism", RFC 2109, February 1997.
[Abine11]	Abine, , "Targeted Advertising Cookie Opt-Out (TACO)", https://addons.mozilla.org/en-US/firefox/addon/targeted-advertising-cookie-op/, February 2011.
[AdBlock-Plus]	AdBlock Plus, , "AdBlock Plus", http://adblockplus.org/en/, .
[AdBlock-Plus-Filters]	AdBlock Plus, , "Writing Adblock Plus filters", http://adblockplus.org/en/filters, .
[Brock11]	Brock, J., "Keep MORE Opt Outs", http://blog.privacychoice.org/2011/01/31/keep-more-opt-outs/, January 2011.
[CDT11]	Center for Democracy & Technology, , "What Does "Do Not Track" Mean? A Scoping Proposal from the Center for Democracy & Technology", http://cdt.org/files/pdfs/CDT-DNT-Report.pdf, .
[DAA10]	Digital Advertising Alliance, , "Opt Out from Online Behavioral Advertising", http://www.aboutads.info/choices/, 2010.
[CDT07]	Cooper, A.L., "Dispelling "Do Not Track" Myths", http://www.cdt.org/blogs/alissa-cooper/dispelling-do-not-track-myths, October 2007.
[Baron10]	Baron, D., "Preventing attacks on a user's history through CSS :visited selectors", http://dbaron.org/mozilla/visited-privacy, April 2010.
[Eckersley11]	Eckersley, P., "What Does the "Track" in "Do Not Track" Mean?", https://www.eff.org/deeplinks/2011/02/what-does-track-do-not-track-mean, .
[EFF]	Electronic Frontier Foundation, , "Panopticlick", http://panopticlick.eff.org/, .
[Google11]	Google, , "Keep My Opt-Outs", https://chrome.google.com/webstore/detail/hhnjdplhmcnkiecampfdgfjilccfpfoe, January 2011.

[Kamkar10]	Kamkar, S., "Evercookie", http://samy.pl/evercookie/, September 2010.
[NoScript]	Maone, G., "X-Do-Not-Track? DNT, c'est plus facile...", http://hackademix.net/2011/01/28/x-do-not-track-dnt-cest-plus-facile/, .
[Mayer]	Mayer, J. and A. Narayanan, "Do Not Track: Universal Web Tracking Opt-Out", http://donottrack.us/, .
[Microsoft10]	Microsoft, , "IE9 and Privacy: Introducing Tracking Protection", http://blogs.msdn.com/b/ie/archive/2010/12/07/ie9-and-privacy-introducing-tracking-protection-v8.aspx, December 2010.
[Mozilla]	Mozilla Foundation, , "Public Suffix List", http://publicsuffix.org/, .
[NAI-History]	Network Advertising Initiative, , "Network Advertising Initiative History", http://www.networkadvertising.org/about/history.asp, .
[NAI-Registry]	Network Advertising Initiative, , "Network Advertising Initiative Opt-Out Registry", http://www.networkadvertising.org/managing/opt_out.asp, .
[NAI-Guidelines]	Network Advertising Initiative, , "Network Advertising Initiative Self-Regulatory Principles for Online Preference Marketing by Network Advertisers", http://www.ftc.gov/os/2000/07/NAI%207-10%20Final.pdf, July 2000.
[Palant11]	Palant, W., "Adblock Plus and (a little) more: Updated roadmap (Adblock Plus 1.3.5)", https://adblockplus.org/blog/updated-roadmap-adblock-plus-135, February 2011.
[PrivacyChoice11]	PrivacyChoice, , "Keep MORE Opt-Outs", https://chrome.google.com/extensions/detail/eoibfeagdaaoimfpfalgbmmegagdconp, January 2011.
[PrivacyChoice-Tracker-Index]	PrivacyChoice, , "PrivacyChoice Tracker Index", http://www.privacychoice.org/companies/all, .
[Soghoian]	Soghoian, C. and S. Stamm, "Universal Behavioral Advertising Opt-Out", https://addons.mozilla.org/en-US/firefox/addon/universal-behavioral-advertisi/, .
[Stamm]	Stamm, S., "Implement do-not-track HTTP header to express user intent to halt tracking across site", http://hg.mozilla.org/mozilla-central/rev/6963333a74d1, .
[Zeigler11]	Zeigler, A., Bateman, A. and E. Graff, "Web Tracking Protection: W3C Member Submission 24 February 2011", http://www.w3.org/Submission/web-tracking-protection/, February 2011.
[Krishnamurthy06]	Krishnamurthy, B. and C. Wills, "Generating a privacy footprint on the Internet. In Proceedings of the ACM SIGCOMM Internet Measurement Conference, pages 65-70, Rio de

	Janeiro, Brazil, October 2006", http://www.cs.wpi.edu/~cew/papers/imc06.pdf, .
[Krishnamurthy09]	Krishnamurthy, B. and C. Wills, "Privacy diffusion on the web: A longitudinal perspective. In Proceedings of the World Wide Web Conference, pages 541-550, Madrid, Spain, April 2009", http://www.cs.wpi.edu/~cew/papers/www09.pdf, .
[Krishnamurthy07]	Krishnamurthy, B., Malandrino, D. and C. Wills, "Measuring privacy loss and the impact of privacy protection in web browsing. In Proceedings of the Symposium on Usable Privacy and Security, pages 52-63, Pittsburgh, PA USA, July 2007. ACM International Conference Proceedings Series.", http://www.cs.wpi.edu/~cew/papers/soups07.pdf, .

Authors' Addresses

Alissa Cooper Cooper Center for Democracy & Technology 1634 Eye St. NW, Suite 1100 Washington, DC 20006 USA EMail: acooper@cdt.org

Hannes Tschofenig Tschofenig Nokia Siemens Networks Finland EMail: hannes.tschofenig@nsn.com