THE DO NOT TRACK FIELD GUIDE

Table of Contents

Section I: Introduction to Do Not Track

Online privacy is a current issue for Internet companies and their visitors. Studies show that privacy concerns are increasing for current users, and that privacy may be a reason people choose not to have Internet access at home.[1] One response to privacy concerns is a Do Not Track (DNT) preference, which lets users indicate they would prefer privacy rather than personalized content. If it is your job to figure out how to honor users' Do Not Track requests within your organization, this implementation guide is for you.

This guide includes three major sections: Immediately below we discuss how DNT fits into the history of Internet privacy. Section two details case studies from four different types of companies; we step through the resources the companies needed and the decisions they made as they implemented DNT, starting on page 12, then conclude that section with a flow chart of decisions for your company to consider during your implementation. Section three provides annotated code samples in a DNT tutorial, starting on page 21; if you are wondering how to detect a DNT header, and what to do about it when you do, this section will give you working code to get started quickly.

BACKGROUND

Rather than issue comprehensive privacy legislation or regulations mandating that companies must not collect or use data in particular ways, the United States largely relies on *industry self-regulation* to protect Internet privacy. Self-regulation groups include the Interactive Advertising Bureau (IAB), Network Advertising Initiative (NAI), and Digital Advertising Alliance (DAA). Internet companies may choose to join one of these self-regulation groups. If they do so, they are bound by the group's rules, but also gain certain benefits. For example, NAI member companies must offer opt-out cookies, and the NAI hosts a centralized page where users can choose to enable them. Self-regulation groups can respond to member companies breaking their rules by revoking membership. The United States' Federal Trade Commission (FTC) is the main source of enforcement for online privacy, and companies have paid millions to resolve FTC actions. The FTC is chartered to

1 85% of parents in the United States say they are more concerned about online privacy now than they were five years ago, according to the preamble of the Do Not Track Kids Act of 2011. Pew found those under 30 are twice as likely to say they can "never" trust social networking sites (28%) than those over 50 (14%) in the United States. Mary Madden and Aaron Smith, Reputation Management and Social Media (May, 2010).
http://pewinternet.org/Reports/2010/Reputation-Management/Summary-of- Findings.aspx?r=1

act when companies engage in unfair or deceptive practices, like when they promise one thing in their privacy policy yet do something else in practice.

Meanwhile, in Europe, the ePrivacy Directive came into force.[2] The Directive has been amended by Directive 2009/136 which changes how some cookies are handled, requiring affirmative consent from users for cookies that are not "strictly necessary". In addition, persistent cookies that contain a unique user ID are classified as personal data. Companies are not sure how to comply with these new regulations without diminishing user experiences online. In part due to these concerns, the cookie directive will not be enforced for a year. Regulators are considering whether DNT could eventually become a mechanism to establish consent to cookies.

Mechanisms for Internet privacy are usually grounded in a theory of notice and choice. As one example, websites offer notice of their data practices through privacy policies, and users choose to visit a site or not. In practice, privacy policies have been unsuccessful in providing clear, usable notice. Unsurprisingly, few users actually read them. This creates *information asymmetries* where the companies offering goods or services know substantially more than the buyer. Economists identify information asymmetries as a market condition in which there is a high likelihood that is better for government to intervene, rather than to rely on a free market solution.

Users have additional choices beyond electing not to visit a specific website. Many advertisers offer opt-out cookies. These allow users to communicate a preference for privacy rather than targeted advertising. The details of what an opt-out cookie actually does, however, vary from site to site. For example, an online behavioral advertising (OBA) company might respond to an opt-out by deleting all existing cookies and setting no new cookies, beyond the opt-out cookie itself. One major search and advertising company responds to an opt-out request by replacing a unique identifier for the user with the string "OPT-OUT." The company continues to collect the same information, but all users who have opted out are aggregated together as if they were one giant user. Another major search and advertising company responds by keeping exactly the same data collection practices, but slightly changing data use. In all three cases, the companies stop showing targeted advertisements based on behavioral profiles. Users have no transparent way to know how their data is collected and used, and in practice, they do not understand what NAI opt-out cookies do.[3]

---

2 See Implementing the EU e-Privacy Directive: The Cookie Problem https://www.cippguide.org/2011/04/12/implementing-the-eu-e-privacy-directive-the- cookie-problem/ for an overview of the EU privacy directives.

3 Aleecia M. McDonald and Lorrie Faith Cranor, "Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising," 38th Research Conference on Communication, Information and Internet Policy (Telecommunications Policy Research Conference) (October, 2010)

Beyond the issue of user confusion regarding what it means to opt-out, opt-out cookies suffer from a technical challenge. Many of the users who set opt-out cookies also regularly delete all of their cookies in order to preserve privacy. This deletes their opt-out cookies as well. There are technical measures to respond to this problem, including the TACO plugin that retains opt-out cookies, as well as a similar solution built into Google's Chrome Web browser. These responses do not work in settings where cookies are not set at all, like on some mobile platforms.

As mentioned above, users also have choices in managing their cookies. Using techniques such as rejecting cookies, using session cookies that only last until the user quits their browser, and employing anti-spyware software that deletes many advertisers' cookies, approximately 30% of US Internet users regularly clear or block cookies. That jumps to approximately 50% in Europe. This reality challenges cookie-based advertising technologies. Some advertisers have moved away from HTTP cookies, using other forms of local storage like LSOs (Flash cookies,) Silverlight, or HTML5. Other advertisers are using techniques like browser fingerprinting or typing patterns to uniquely identify users without using local storage. IP address is a quasi-stable identifier, and on all but new versions of Windows, IPv6 includes MAC addresses (hardware-based permanent unique identifiers) as part of the user's IP address by default. Most modern mobile devices have unique identifiers. This means that even users who set opt-out cookies, delete other cookies, and read privacy policies may still not have transparency or control over their data privacy. With technologies that do not rely on local storage, users are particularly unlikely to know what data is being collected about them, by whom, or how it is being used. Since the notice and choice approach requires transparency to work — and, if the US is to continue with a self-regulatory approach — then we require new tools to empower user control.

In January of 2011, FTC staff members issued a draft report endorsing Do Not Track as one possible new approach.[4] The FTC report states that current industry self-regulation efforts in the U.S. are not enough to avoid increased regulation or legislation. The DNT idea started in 2007, and has changed substantially since.[5] As an alternative to new legislation, the FTC report suggested that industry devise a DNT mechanism that allows users to opt out of data collection and use.

In their next Web browser releases after the FTC report, both Mozilla Firefox and Microsoft's Internet Explorer implemented a DNT feature in the spring of 2011, and shortly after added support for mobile browsing on Android. Apple's Safari web browser added support

4 Federal Trade Commission, "FTC Staff Issues Privacy Report, Offers Framework for Consumers, Businesses, and Policymakers," http://www.ftc.gov/opa/2010/12/privacyreport.shtm (January 1, 2011).

5 For one account, see Christopher Soghoian's "The History of the Do Not Track Header," http://paranoia.dubfire.net/2011/01/history-of-do-not-track-header.html (January 21, 2011)

for Do Not Track in the summer of 2011. By 2012, we expect that approximately half of Internet users will have upgraded to a modern Web browser that supports DNT. All three browser implementations have different user interfaces for users to enable DNT, but all three respond in the same way on the back end, sending the same message to websites.

Although three browsers elected to implement sending the same DNT signal, they could diverge in the future. To ensure DNT means the same thing regardless of which browsers and websites are involved, two different standards bodies have discussed DNT — the IETF and the W3C. As of summer 2011, it appears W3C will take the lead on DNT standards. If your company is interested in following or participating in DNT standards, you might consider subscribing to W3C mailing lists to keep up-to-date.[6]

Do Not Track is being discussed primarily within the United States at this time. Presumably this will change, both because W3C is an international standards body, and because European companies face pressure to find technical means to comply with the ePrivacy Directive and opinions of the Article 29 Working Group. European privacy requirements around notice and consent are undergoing rapid change.

HOW DO NOT TRACK WORKS

At its most basic, DNT is a preference expressed by users. DNT lets you hear directly from your users that they have privacy concerns and they would like your site to respond to those concerns.

At a technical level, DNT is an HTTP header.[7] When DNT is enabled, Firefox sends the string "DNT: 1" for each browser transaction (for example, to load a Web page, an image, a widget, or other subpart of a page).

Here are two different ways you can see DNT in action from the Firefox browser.

In DNT's debut in Firefox 4.0, under **Firefox → Preferences... → Advanced → General** there is an option labeled "Tell web sites I do not want to be tracked." Checking this box

6 For a summary of the first W3C workshop, see http://www.w3.org/2011/track- privacy/report.html

7 HTTP headers contain information sent prior to the content. For example, HTTP headers may contain information about the referring website visited prior to the current site, the user agent string containing the operating system and Web browser requesting content, etc. The Internet Engineering Task Force (IETF) first standardized HTTP headers in RFC 2616 and they have been modified several times with additional extensions. DNT is currently an optional HTTP header; user agents like Web browsers may choose to implement DNT, but are not required to.

turns on DNT. Unchecking it stops sending a DNT header. This is the interaction users have with DNT in Firefox. (See Figure 1 below).

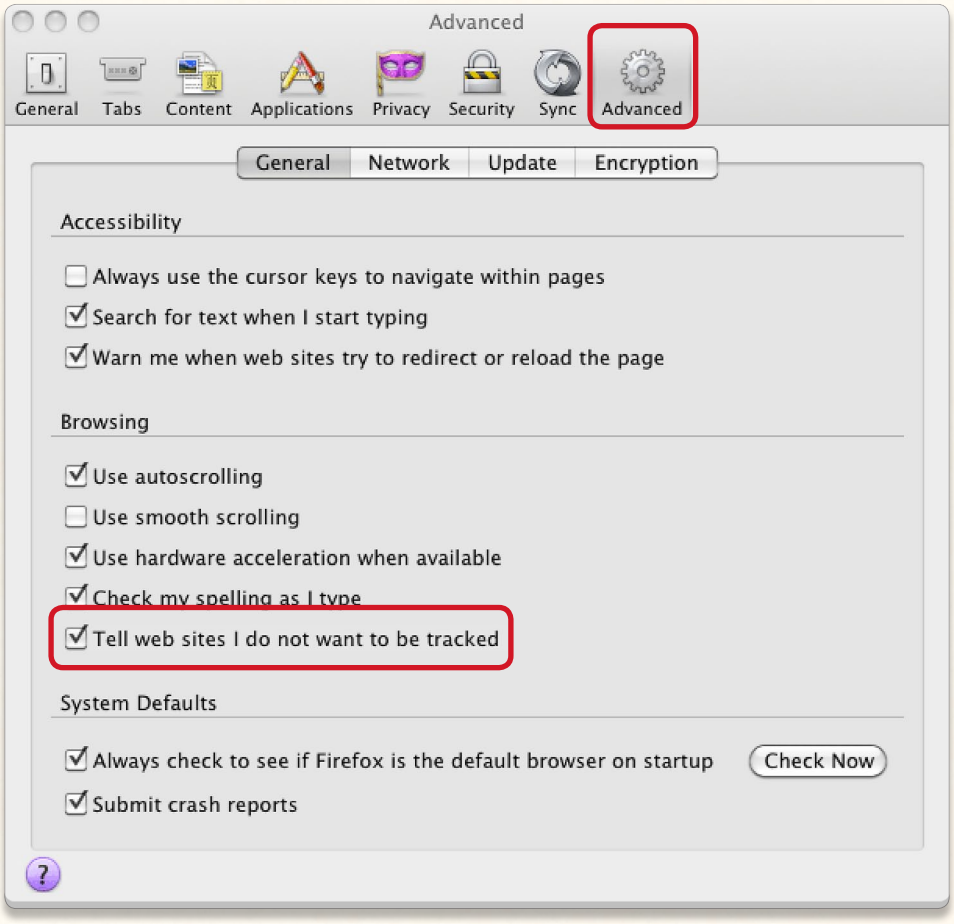

Figure 1: *User interface for Do Not Track in Firefox 4.0*

In Firefox 5.0 and later, the same checkbox is under **Firefox ➔ Preferences... ➔ Privacy.** (See Figure 2 below).

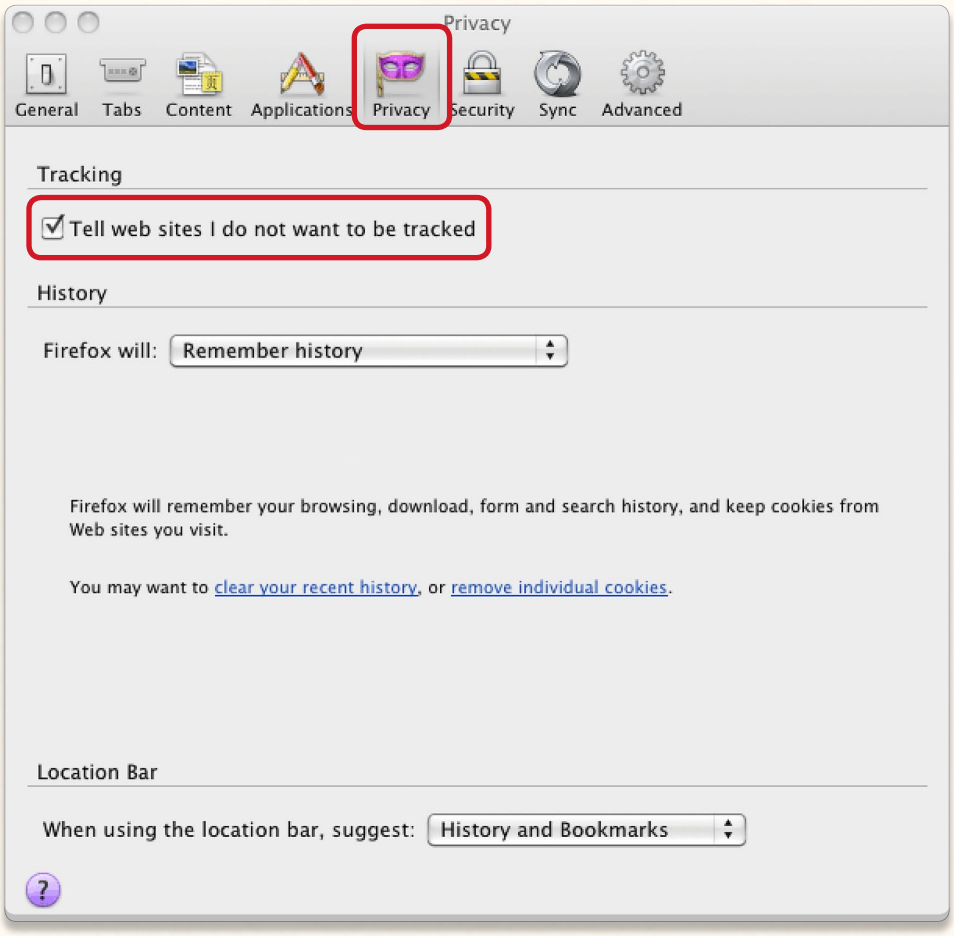

Figure 2: *User interface for Do Not Track in Firefox 5.0*

In Firefox for mobile, users can also enable DNT under **Options → Privacy**, where there is a similar option labeled "tell sites not to track me." Checking this box turns on DNT so the header can be sent to sites you browse from your Android or Maemo mobile devices. (See Figure 3 below).

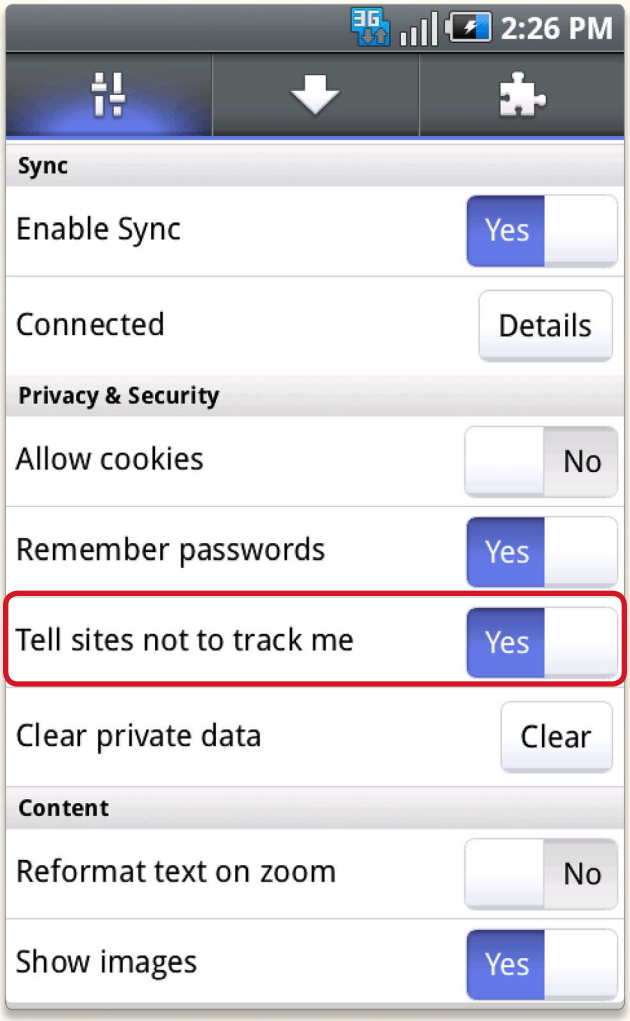

Figure 3: *User interface for Do Not Track in Firefox Mobile*

You can watch Firefox send HTTP headers, for example with the Live HTTP headers plugin. The example below shows the HTTP headers Firefox sent while loading wikipedia.org, with the DNT header highlighted in yellow for clarity.

```
GET / HTTP/1.1
GET / HTTP/1.1
Host: www.wikipedia.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.6;
rv:2.0.1) Gecko/20100101 Firefox/4.0.1
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
DNT: 1
Connection: keep-alive
If-Modified-Since: Mon, 23 May 2011 07:29:40 GMT
HTTP/1.0 304 Not Modified
Date: Wed, 25 May 2011 03:53:03 GMT
Content-Type: text/html; charset=utf-8
Last-Modified: Mon, 23 May 2011 07:29:40 GMT
Age: 7
X-Cache: HIT from sq73.wikimedia.org
X-Cache-Lookup: HIT from sq73.wikimedia.org:80
Connection: keep-alive
```

If users check the “Tell web sites I do not want to be tracked” box, then Firefox sends out the HTTP header “DNT: 1” to websites. Do Not Track is that simple.

WHAT DOES TRACKING MEAN?

Where Do Not Track gets complex is in deciding what actions to take when your website receives a DNT header. This guide does not attempt to define tracking, nor does it proscribe what it means for your site to comply with an incoming DNT header. The purpose of this guide is to help you understand some of the common choices available to you, so that you can make the best decisions for your site and your users.

There are many different definitions of tracking that have been published. You may find it useful to read some of the additional resources at the end of this document. For example, some advertisers are calling for “Do Not Target” rather than “Do Not Track,” allowing data collection to continue unchanged. However, the original FTC staff document called

for limitations of data collection, not just data use, after users express a Do Not Track preference. FTC Commissioners and staff continue to discuss Do Not Track as pertaining to both data collection and use.

Another point of contention is whether DNT applies to first-parties as well as third-parties, plus disagreement on what a first-party is. For example, are widgets like the Facebook Like button first-party or third-party? Are analytics companies bound by that are contract not to use data beyond analysis for their clients to be treated like first-parties?

Even with the contours of DNT agreed upon, different parties call for a variety of exemptions. For example, financial companies want to collect and use data for fraud prevention, even for users signaling DNT. Other possible exemptions that companies have requested include billing for ads, analytics, ad rotation or frequency capping, research and development, federated login, and to provide data to law enforcement.

Early research shows that users expect DNT to be broadly defined across first- and third-parties, that it would include data collection as well as data use, and that they would be surprised by exemptions, with the possible exception of fraud prevention and law enforcement.[8] The more broadly you define DNT, the more likely you are to meet your users' expectations and earn their trust.

PRIVACY TECHNIQUES AND DO NOT TRACK

Users have many privacy tools including setting opt-out cookies, using browser settings to enforce session cookies or blocking cookies entirely; ad blocking plugins that prevent content from loading; and Tracking Protection Lists (TPLs) in Internet Explorer. These are all unilateral actions taken by users, sometimes not based on an understanding of how the Internet works. DNT allows users to express their intentions and their desire for privacy. DNT also moves beyond cookie-based approaches. For example, DNT might affect a company that fingerprints users' browsers or uses other forms of local storage, like Silverlight or LSOs (sometimes referred to as "Flash cookies" by the press.) Rather than needing to understand how these technologies work, users can enable DNT to signal a preference once and let companies determine how best to respond to that request.

8 McDonald, Aleecia M., and Peha, Jon M. User Expectations for Do Not Track. *39th Research Conference on Communication, Information and Internet Policy (Telecommunications Policy Research Conference)* September 23-5, 2011, in preparation.

Implementing DNT complements other self-regulatory mechanisms, and is not a replacement for your current investment in self-regulatory approaches. Privacy is a very nuanced, individual topic. Different users will be comfortable with different ways to manage their data. DNT gives them another way to voice their choices, and gives you another way to understand your users' preferences.

PRIVACY POLICIES

Your privacy policy may be a good place for you to acknowledge users who have DNT enabled. You could put a banner at the top or bottom of the policy, or a graphic off to the side, calling attention to your support for DNT. It is a good practice to clearly explain what you change when you see DNT, both in terms of data collection and data use. One company today has coded its privacy policy site to change dynamically to signal support for DNT when a visitor with the header enabled visits the privacy policy.[9]

The disadvantage of communicating via privacy policies is that few people read them. You might consider other ways to communicate with users, too, based on what you know of your site use patterns, and whether there are specific areas where privacy concerns are likely to be heightened.

OPT-OUT COOKIES AND AD CHOICE

Opt-out cookies and the Ad Choice campaign[10] are complementary to Do Not Track. You may encounter users with 1) DNT on but no opt-out cookies, 2) DNT off but opt-out cookies, or 3) both DNT and opt-out cookies. In all three cases we suggest that you treat this as a decision from the user that they do not want to be tracked on your site. The majority of your users will have neither DNT on nor opt-out cookies set, in which case you can respond with your normal practices.

DO NOT TRACK AND THE LAW

There is no explicit regulatory requirement in any country that mandates implementing support for the DNT header. That said, there are legal and compliance-related considerations to keep in mind when designing how to support consumer requests not to be tracked online via browser-based DNT mechanisms.

---

9 See http://www.chitika.com/privacy

10 Ad Choice puts an icon on ads. Users can click the icon and navigate to a page that lets them view and set opt-out cookies for different advertisers. In Europe, so far this is not seen as a viable alternative to affirmative consent to cookies. See http://www.aboutads.info/

The self-regulatory program being proposed by the online advertising industry currently does not include support for DNT, as implemented by browser manufacturers. In the United States, supporting members of the DAA and the IAB are required to offer an opt-out mechanism, but the program does not require support for the DNT header at this time.

Supporting DNT has legal considerations, as it may extend a site's compliance requirements beyond what is included in its current privacy policy. In the US, saying that a site supports DNT now means that the site must comply with that commitment across its sites and in a manner that is consistent with the site's definition of what DNT means for its site and the expectations of its consumers.

Regulation may emerge, as early as 2012, if industry doesn't show that it can support DNT on its own and/or current policy makers in the US and Europe aren't successful with their proposals. In the United States, several commissioners and the chairman of the Federal Trade Commission have called for a Do Not Track system. Several legislative proposals have also been submitted at the state and federal levels that call for the creation of DNT. In Europe, a few policy makers at the national and country level have started to endorse the idea of DNT, including the Minister of the Department of Media, Culture and Sport in the United Kingdom and the Vice President of the European Commission's Digital Agenda. Both policy makers are pushing for DNT support by mid-2012.

Please consult with your legal and privacy teams to weigh the regulatory and compliance risks associated with implementing support for Do Not Track.

Section II: Case Studies

We spoke with several companies about their DNT implementations. We've summarized their experiences into four case studies that may be useful to you as you plan your approach.

CASE STUDY 1: ADVERTISING COMPANY

We spoke with the engineer who implemented DNT at an advertising company. He came to work one morning, read about DNT in Slashdot, and wrote a few lines of code. Start to finish, the implementation took approximately thirty minutes of his time. The advertising company already had an existing code base to support opt-out cookies so they were able to reuse existing code.

When they detect a DNT header from a user, they perform the following steps:

1. Set the content of their remarketing cookies to an empty string. This removes all identifiable data from the cookie at once.
2. Set the expiration date for the user's cookies to a time in the past. This deletes their cookies the next time the user requests the page, which may not happen immediately.
3. Their existing code logged every time they could not set a cookie, as well as every time they detected an opt-out cookie. They added a new category for every time they detect a DNT header. This logging happens based on which branch of their code executes, and is not tied to any user information. As a result they cannot tell how many unique users have DNT turned on, but they know what percentage of their traffic involves blocked cookies, opt-out cookies, or a DNT header.
4. They do not set a new opt-out cookie. They reasoned that anyone with a DNT header probably also manages their cookies. An opt-out cookie would either not be set at all, or would be deleted quickly. They do use all of the same code already in place when they read opt-out cookies, and treat DNT just like an opt-out cookie.
5. If a user is viewing the privacy policy with a DNT header on, they communicate directly with the user. They conclude their privacy policy with a colored box addressed to DNT users, confirming the ad company received the DNT header and will not track the user. They also remind users that DNT applies to each browser, so users may need to set DNT in multiple places. This again parallels their opt-out cookie support. Without a DNT header, users see a colored box that reports whether they have opt-out cookies or not, and includes a button to opt out if there is no opt-out cookie set.

The advertising company considered implementing DNT a "no brainer" because it was straightforward to code and gives users another way to express privacy choices. As an ad network they already had done the work to support opt-out cookies, so DNT was easy to add. The ad company sees DNT as just one more form of communication with their users. They decided there was no reason to wait to implement DNT when they could handle it so quickly and demonstrate commitment to supporting users' privacy choices.

CASE STUDY 2: TECHNOLOGY PROVIDER

We spoke with a company that is currently designing their DNT support. This company works with DSPs, ad networks, and others as clients for targeted advertising, as well as providing fraud detection services. The technology provider uniquely identifies users through a variety of means, including browser fingerprinting, which is not cookie-based.

The company told us they are interested in DNT because it is a persistent way for users to express preferences and to opt-out permanently. Cookie-based solutions become difficult to explain, with users trying to clear cookies for privacy yet keep opt-out cookies at the same time. The company is particularly interested in being able to communicate with users, to give notice of business practices, and then provide a choice mechanism. They have already built a platform to allow users to opt-out of some data collection and use, and they are currently implementing all DAA requirements so they can join the DAA opt-out page as well.

One of the advantages to their pre-existing solution is that it is flexible: Users can opt out of some clients but not all. In contrast, DNT is currently a single signal that users do not want to be tracked, and does not allow users to make individual exceptions on a per-company or per-advertiser basis. The company concluded that DNT's advantages make it worthwhile to implement now, while being engaged in DNT innovation and standards in the future.

When they detect a DNT header from a user, they expect to perform the following steps:

1. Stop collecting and using data for third-party OBA.
2. Continue to collect and use data for fraud prevention.
3. Largely continue to collect and use data for first-party analytics and customer recognition. They will offer their customers the option to interpret DNT to mean no first-party collection and use at all, or not, and it will be up to each advertising

> network to choose. Each ad network must have a privacy policy that discusses how they interpret Do Not Track and clarifies to what extent they support the DNT header. In some cases opt-out cookies will conflict with the policy of ignoring DNT for first-party, if a user has a specific opt-out cookie for the advertising network. In that case the opt-out cookie will be honored.

This company's approach to ignoring DNT for fraud prevention is likely to be less controversial than the final point on first-party use. The idea that users must have both opt-out cookies and DNT on to be fully protected may cause consumer backlash, depending on whether users think DNT applies to first parties or not, and whether they think first-party status extends to business partners.

In addition to responding to the DNT header, the company is adding more feedback for DNT users on its own preferences page, where they currently manage user opt-outs. When a DNT-enabled user visits the preferences page, the user will see an acknowledgement that DNT is on, plus an explanation of which data practices are — and are not — affected by the DNT signal (e.g. fraud prevention). The technology company is considering passing information about DNT to clients via API calls, but that is not certain yet. They also hope to be able to help their clients have conversations with users who have TPLs or DNT on to explain to the end user what the data practices are, and see if users are interested in opting back in.

CASE STUDY 3: MEDIA COMPANY

We spoke with a media company that has a large portfolio of intellectual property. They keep statistics on the popularity of their offerings, which are accessible through partner websites. The company was very happy to adopt DNT because they like a privacy signal that is not tied to cookies. The media company already had extensive infrastructure for opt-out cookies in place, with a central location to opt out of partner sites, and they were able to leverage that for supporting DNT. It took one engineer a few hours to complete their DNT implementation.

When they detect a DNT header from a user, they perform the following steps:

1. Stop setting any new cookies for that user.
2. Continue to count the aggregate number of visits to a given media offering, but for DNT users they do not count unique visitors.
3. Clear all data in their cookies.
4. Set the cookie expiration date to the past so the cookie will be deleted.

Initially, the media company treated Do Not Track more like a pause button than a stop button, in that they did not delete information they stored in users' cookies. This way if a user was only experimenting with DNT and later turned DNT off, the media company would recognize them again and resume normal practices. A blogger performing Web forensics raised concerns when he noticed that the media company advertised DNT support, yet kept information stored in cookies. It can be difficult to convince users that even though users see your cookie on their hard drive, you are not reading it. In the end, the media company decided it was easiest just to delete the cookies for DNT users rather than try to explain the nuance of their initial implementation, and they revised their approach to the one we outlined above.

CASE STUDY 4: SOFTWARE COMPANY

We spoke with a software company that is not involved in advertising, but they are currently in the process of implementing Do Not Track. Two people from the legal department sat down with the company's privacy policy and began the process of understanding how DNT would affect them.

First, they created a table of all of the product lines they offer. They classified them by products that can see a DNT header and those that cannot (for example, a stand-alone desktop application is not affected because it cannot read a DNT header). For those products that do see a DNT header, they then looked at the details of the product offering. In a few cases they decided it did not make sense to honor a DNT header. For example, they have a small research group with projects of fewer than 100 people, where the point is to get feedback from customers. Customers understand they are sending a great deal of data, including stack traces or debugging information. In this case they decided the appropriate action was to add a note to the top of the download page, visible only to users with Do Not Track enabled. They remind DNT users that despite their preference to avoid tracking in this case their involvement requires data collection and use, and to please not

take part in the research if they are not comfortable with that. In other cases, the legal team took notes of which projects they need to investigate further, and which engineers to speak with. They are going to approach project leaders one-by-one to determine the best way to respond to DNT for any given product.

Second, they created a list of "hot spots" of areas to watch for in all products. These were:

- IP logging
- Email containing HTML beacons
- Internal website metrics
- External analytics vendor

Their analytics partner offers an opt-out cookie, but does not support DNT at this time. They determined they will need to require any analytics partner to honor DNT in the future, and added that to the list of points to negotiate when their contract comes up for renewal in a few months. For the remaining three areas, they will contact the engineers involved to speak about how they collect and use data, and determine the best way to respond to DNT. These issues cross product lines.

ADDITIONAL ISSUES TO CONSIDER

While speaking with companies that have implemented DNT or are in the process of doing so, we also heard of a few other decision points that may apply to your company. NAI members and other companies offer opt-out cookies; IP addresses are uniquely identifiable but easy to forget because they are not usually part of cookie data; mobile devices have additional sources of private data; and for a few companies it is important to think about how to manage third party cookies that are set as if they are from first parties.

OPT-OUT COOKIES

One company planned to implement DNT by deleting all cookies they set, and then they realized this would also include any opt-out cookies for their site. They elected to make an exception and leave opt-out cookies. This way if users experiment with DNT and turn DNT off, the users will not have to set all of their opt-outs again. This is a conservative approach that respects user choice, and is easy to explain.

IP ADDRESSES

At the time of writing, the United States Senate is about to consider new laws mandating data retention for IP addresses and other information. In the future, multi-national companies may find that the US and EU regulations conflict. You might want to review the current status of legal requirements and prohibitions as you consider your options with IP addresses. There are three approaches we have seen companies take:

1. Continue to collect IP address in server logs, regardless of DNT status. In some cases this is simply oversight, since server logs are not cookie-based and may not immediately come to mind as a form of tracking users. However, European Union nations classify IP address as personally identifiable information, and EU visitors may have a strong expectation that their IP addresses are not logged.

2. Truncate IP addresses in server logs by dropping the last octet of the address (so, for example, 128.2.45.67 and 128.2.45.68 both become the truncated 128.2.45, and the two IP addresses become indistinguishable.) The idea here is generally that because there may be 255 computers with the same first three octets for their IP address, truncation should provide some privacy. At the same time, companies can still use truncated IP addresses for geoIP to understand where their customers are physically located. Truncation is not anonymity. Especially in small datasets, there is a good chance of unique or very few users matching the truncated IP address. If your only other choice is to store the full IP address, truncation is a modest step toward protecting user privacy.

3. Do not log IP addresses. It is technically easy to set Apache or IIS to not record the IP addresses of visitors who had DNT enabled. We have not tested it, but sample code is available from http://donottrack.us/server.

MOBILE DEVICES

Firefox supports sending a DNT header on a mobile device, for example, from Firefox on an Android cell phone. If you have a version of your website optimized for mobile device users, you can implement support for Do Not Track for your mobile website too.

DNT for mobile devices works the same way as DNT for browsers not designed for mobile devices: when users turn DNT on, their browser sends “DNT: 1” as an HTTP header. Mobile web browsing is affected, but mobile applications that do not use HTTP are not affected.

If you collect information that is not available from desktop computers (for example GPS-

based geolocation, serial number, UDID, or any device-specific identifiers) you might want to think about how to limit that collection for DNT-enabled visitors.

THIRD PARTY COOKIES IN A FIRST PARTY CONTEXT

In general, you can only read, modify, or delete cookies that you set. However, some advertising companies are setting their cookies on a first party site as if the advertising companies were the first party. There situation pertains to a very few companies; if yours is not one of them, you can skip this section.

As an example of what we mean by a third party cookie set as if it were a first party cookie, imagine user Alice visits website MyNews.com which serves an advertisement from a company called Adverts. She might get cookies from multiple hosts, for example *mynews*, *www.mynews*, and *adverts*. We would expect to see first party cookies in *mynews* and *www.mynews*, and third party cookies in *adverts*. However, there are a few companies that serve their third party cookies in a first party way, for example an advertising cookie from Adverts set on the mynews host. Several companies offer this functionality. Google analytics is a prevalent example.[11] We use them throughout this section, though we did not speak with Google about their practices.

We spoke with an advertiser that sets third party cookies in a first party context. When they receive a DNT header, they want to make sure they delete all of the cookies they set. However, because they are setting cookies like a first party, they have access to more than just the cookies they write themselves. For example, if an advertising company sets first party cookies on the mynews host, that means they can also delete any other cookies set on mynews — including cookies set by MyNews and even by competing advertising companies that also are setting third party cookies in a first party context. If Adverts decided to delete all cookies they have access to, they could also delete any Google Analytics cookies plus all first party cookies. This could happen even if Google did not honor DNT and the first party did not honor DNT.

While Mozilla does not wish to define tracking, this is one area where we will express an opinion. It is probably not a good practice to delete competitor's cookies in the name of DNT. We suggest that you only delete cookies you set, even if you have access to other cookies that are also third party cookies in a first party context, or classical first party cookies set by a first party.

---

11 See "How does Google Analytics work?" http://www.google.com/support/analytics/bin/answer.py?hl=en&answer=55539 and "Cookies & Google Analytics" https://code.google.com/apis/analytics/docs/concepts/gaConceptsCookies.html

An advertising company wanted to honor DNT headers in the following way:

- Do not delete any cookies set by another party
- Do not delete any opt out cookies
- Delete all cookies the advertising company set

This sounds simple. The advertising company sets four cookies with known names. All they have to do when they see a DNT header is to delete those four cookies. However, there was one added bit of complexity. The advertising company exposes an API to their customers, which enables their customers to write their own advertising cookies in the same directory. The advertising company has no way to know what names their customers use for any cookies set through this API. As a result, the advertising company cannot delete all cookies associated with their product, because they do not know what their customers' cookies are called, and they cannot delete all cookies without deleting cookies from other parties.

Moving forward, the advertising company is considering a preface for all of their cookies, so they can delete all of their cookies that begin with their preface. Even after they deploy this new system, they will still have "legacy" cookies their customers set through the API. Eventually all of those cookies will expire, but that will take time. Until then, they could attempt to get a list of all customer cookie names and hard code those into their DNT response. Or they could encourage all of their customers to migrate cookie data to the new naming convention. Neither of these is a perfect solution.

CASE STUDIES FLOW CHART

While the case studies above are all different, some common decision points emerged. We have also discussed some points to consider with companies we did not profile, including DNT on mobile devices. You might want to think about the issues outlined in Figure 4 as you plan your implementation.

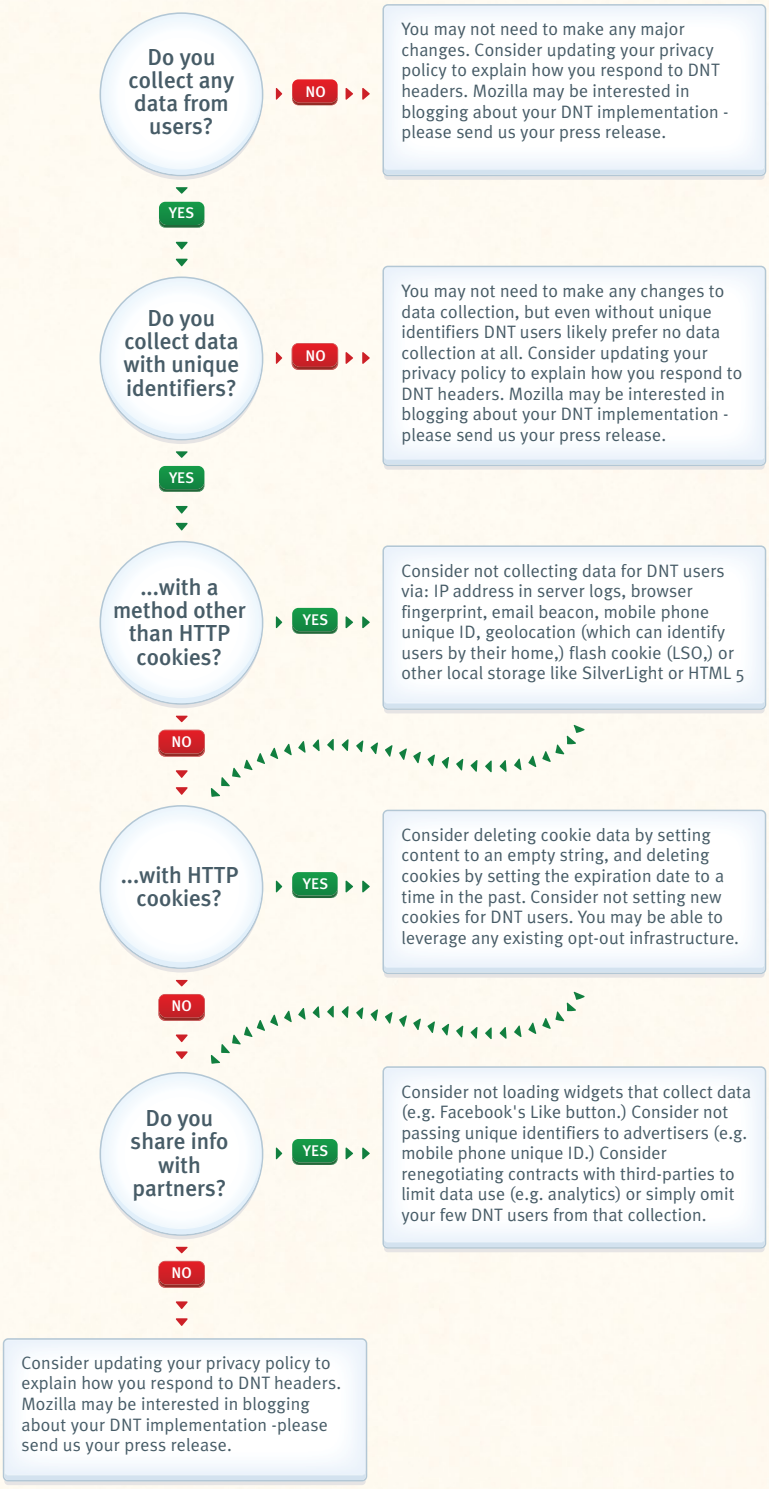

Figure 4: *Case studies flow chart*

Section III: Tutorials

Working with the Do Not Track header is fairly easy on a technical level. In the following tutorials we provide sample code to get you up and running quickly. You can download this sample code from Mozilla at http://dnt.mozilla.org.

We expect most readers are familiar with JavaScript. You cannot use JavaScript to read the Do Not Track value straight out of the HTTP header. We provide PHP code to set a variable in PHP, and then show you how to call the PHP code from JavaScript. You could just as easily implement this in Ruby or other languages if you prefer not to use PHP, in which case the PHP code should give you a good starting point for the logic involved. **REQUIRED:** You must run this PHP code (or something similar) on your Web server or you will not be able to read the Do Not Track header. You may need to install PHP on your Web server if it is not already installed.

Right now, when users enable the DNT header they can only set it as always on, and cannot specify if there are any companies they want to exempt. However, in the future, that may change. **SUGGESTED:** Also store and run any JavaScript code on your web server. Otherwise, if your JavaScript code is on a different server from the PHP code, you run the risk of getting a DNT value from the server the JavaScript runs on, not your main server. That would test fine today, but could break in the future if DNT changes. If for some reason you must run your JavaScript on a different server, you can put more logic into the PHP code on the main server.

Below you will find code for three tutorials:

1. Tutorial 1 is the “Hello, World” for DNT. We show you how to read a DNT header from website visitors, and how to pop up an alert to display the value of that header.
2. Tutorial 2 moves beyond a quick alert and instead displays an image that changes based on the user’s DNT settings. This is something you might use in practice to communicate with your site’s visitors. We introduce one bit of complexity: how to handle the possibility that users changed their DNT status after caching one of the images.
3. Tutorial 3 illustrates how you could aggregate user data, or delete cookie data and expire cookies.

TUTORIAL 1: READING A DNT HEADER

Most programming language tutorials start off with a "Hello, World" program to confirm you have the programming environment set up correctly. With DNT, the first thing you may want to do is confirm that you are able to successfully read an incoming DNT header.

This tutorial introduces two files, a PHP file we named `intojs.php`, which reads the DNT value, and some sample JavaScript that displays the DNT value in an alert in a Web browser.

PHP FILE

First, the PHP file. You can download the sample code from Mozilla <http://dnt.mozilla.org>, or copy and paste this straight into a file named `intojs.php` saved on your Web server:

```
<?php
// filename: intojs.php
// dnt detection script
// Grabs the HTTP DNT request, sets the window.isDntOn variable so it
// can be checked from JavaScript code.

function getDntStatus() {
   // Handy to have as a function because you may use this a lot.
   // The important logic here is: Dnt can be on (1), off (0), or
   // unset. You want to make sure you account for unset so you do
   // not de-reference a null pointer somewhere in your code.
   // returns TRUE if Dnt is on and is equal to 1,
   // returns FALSE if Dnt is unset or not equal to 1.
   return (isset($_SERVER['HTTP_DNT']) && $_SERVER['HTTP_DNT'] == 1);
}

// set PHP to send javascript output to the browser
header("content-type: application/x-javascript");

if (getDntStatus()) {
   echo "window.isDntOn = true;";
} else {
   echo "window.isDntOn = false;";
}
?>
```

JAVASCRIPT FILE

Second, in a JavaScript file, perhaps called `hello.html` and also stored on your Web server, paste the following:

```
<html>
   <body>
      <script src="intojs.php"></script>

      <script>
         alert("Hello world! DNT is set to: " + window.isDntOn);
      </script>
   </body>
</html>
```

There are only two lines of content. In the first, we call code in the `intojs.php` file you created above. This assumes the JavaScript file is in the same directory as `intojs.php`, but you could use a relative path if it is not. You could also use an absolute path to point to code on a different server, but as we explain at the start of the tutorial, we recommend against doing so.

The main content of this JavaScript file is to create an alert and display a message to see if DNT is set to `TRUE` or `FALSE`, using the value of the `window.isDntOn` variable you created in `intojs.php`.

TESTING THE TUTORIAL

Once you have the PHP and JavaScript files in place, start a Web browser and visit the `hello.html` file. You should see an alert that accurately reports if you have DNT on or off in that browser.

Here are some browser configurations you might want to test:

- Firefox 4.0 or 5.0, no DNT setting. Should return `FALSE`.
  (may require re-installing Firefox if you have already set the DNT preference)
- Firefox 4.0 or 5.0, DNT off. Should return `FALSE`.
- Firefox 4.0 or 5.0, DNT on (Preferences ➔ Advanced for 4.0, Preferences ➔ Privacy for 5.0). Should return `TRUE`.

- Internet Explorer 9.0, tracking protection lists off. Should return `FALSE`.
- Internet Explorer 9.0, with a tracking protection list. Should return `TRUE`. (To test: Visit dnt.mozilla.org with IE and enable an empty TPL.)

Firefox 4.0 and 5.0 should work identically, so there is no need to test more than one.

TUTORIAL 2: DISPLAYING DNT STATUS WITH CACHING

While useful for testing, you probably do not want to pop up alerts when DNT is detected. You might want to show a graphic, however, to assure visitors that DNT is being honored. We do something along those lines at <http://dnt.mozilla.org>.

Structurally, this is very similar to detecting a DNT header and displaying an alert. The main difference is that images get cached. If you have a graphic to show DNT status, you will want to ensure you do not cache it, so that you do not display an out-of-date image.

We used one PHP file, one HTML file, and two image files. The main file:

```
<?php
// Save as: dnt_status.php

// dnt detection script
// Grabs the HTTP request (i.e., cookies and DNT header and referrer)
// then serves an appropriate image back.

$dnt = isset($_SERVER['HTTP_DNT']) and $_SERVER['HTTP_DNT'] == 1;

// Force no-caching
header("Expires: Thu, 19 Nov 1981 08:52:00 GMT"); // use any old date
header("Cache-Control: no-store, no-cache, must-revalidate,
postcheck=0, pre-check=0");
header("Pragma: no-cache");

// serve the appropriate image.
header("Content-Type: image/png");
if($dnt) {
   readfile("images/DNT-indicator-on.png");
} else {
   readfile("images/DNT-indicator-off.png");
}
?>
```

This returns either the image file for users with DNT on, or the image file for users with DNT off, which we stored in `images/DNT-indicator-on.png` and `images/DNT-indicator-off.png`, respectively. (You will need to create image files for your site, perhaps something as simple as a checkmark and an X while you test.)

And we invoke the `dnt_status` code from a third file, in our case `index.html`:

```
<html>
<head>
<title>Do Not Track graphics</tile>
</head>

<body>
<img style="border:1px solid blue;"
   src="/dnt_status.php"
   alt="Do Not Track Indicator"
   title="Do Not Track Indicator."/>
</body>
</html>
```

TUTORIAL 3: COLLECTING AGGREGATE DATA BASED ON DNT

As we detail in the case studies, there are many different approaches you might take to responding to a DNT request. Below, we give an example of how you might set a cookie to aggregate user data rather than collect it on a per-user basis. Please understand this sample code is not meant as an endorsement of data aggregation as an approach to DNT. In particular, it may not meet your users' expectations for what DNT means, and we encourage you to think carefully about which approach to pursue. However, data aggregation is one approach already used in practice. For example, Google handles opt-outs by setting a cookie containing the string OPT-OUT for all users. The sample JavaScript code below follows that general approach.

The sample JavaScript code below also gives a starting point for how to delete and expire cookies based on DNT status.

```
// portion of a JavaScript file to set opt-out cookie
// assumes intojs.php file from first tutorial.

function setCookie(cookie_name, string_value, time_to_expire)
{
   // it is likely you already have something implemented you
   // can use. If not, there are many examples online
}
```

```
if (getDntStatus()) { // If you detect a Do Not Track header...
   deleteAllCookies(); // Write this code to delete cookies
   setCookie('trackingcookie', "opt-out", time() + 60*60*24*365*5);
   // sets the value of trackingcookie to opt-out for all DNT
   // users, with an expiration time of 5 years (in seconds)
} else {
   // current code for tracking goes here
}
```

For users with DNT, first you need to delete the tracking cookies you already have on their computers. (If you are not sure which cookies you set, you might consider deleting all cookies, since you can only delete your own cookies.) Otherwise you will run into the problem that you set a DNT cookie, yet still have tracking cookies saved, which is bound to confuse a few savvy — and potentially vocal — users. If you store keys into a backend database, you may wish to delete information from your backend database now, before you delete the key and then have stored information you will never retrieve again. (If the current IETF draft on DNT is adopted, as per section 8.1, all third-party tracking data must be deleted, not just data in cookies.) Also think about any non-HTTP cookie tracking you may store on users' hard drives, such as LSOs, cache cookies, HTML 5 local storage, Silverlight local storage, and so on. If you only delete HTTP cookies and leave other local storage behind, people may think you are not honoring DNT.

After deleting existing tracking cookies, if you are going to collect aggregate data, you might set a new cookie with the value of `opt-out` or something similar. All DNT users will share a common identifier of `opt-out` rather than a per-computer identifier. In our code example, we set the expiry time for the opt-out cookie to five years. You are free to choose any length of time you wish, but note that self-regulation principles require opt-out cookies to last at least five years. It is probably good practice to pick a time that is at least as long as any tracking cookies you set.

Additional Resources

For additional history, context, and ideas of what Do Not Track means to various stakeholders, please refer to the following:

- The FTC's staff report that calls on industry to create a DNT mechanism http://www.ftc.gov/opa/2010/12/privacyreport.shtm
- FTC guidelines for behavioral targeting http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf
- The Do Not Track Cookbook contains approaches to data collection in DNT-friendly ways, http://donottrack.us/cookbook.
- The original IETF proposal for Do Not Track, http://datatracker.ietf.org/doc/draft-mayer-do-not-track/
- The Electronic Frontier Foundation (EFF) discussion, https://www.eff.org/deeplinks/2011/02/what-does-track-do-not-track-mean.
- The Center for Democracy and Technology (CDT) DNT proposal, http://fec.cdt.org/DNT-2.
- Materials from the W3C workshop on DNT, http://www.w3.org/2011/track-privacy/