Title: Community Group comments on W3C DNT

Date: Jan. 8, 2012

Editors: Lee Tien (EFF) and John M. Simpson (Consumer Watchdog)

This draft document represents the current consensus views of the following organizations: ACLU, Center for Digital Democracy, Center for Media and Democracy, Consumer Federation of America, Consumers International, Consumers Union, Consumer Watchdog, Electronic Frontier Foundation, Fundacja Panoptykon, Privacy Rights Clearinghouse, and World Privacy Forum. Other consumer and privacy advocacy groups are considering the draft and are likely to join. We have reacted to the W3C Tracking Protection Working Groups First Public Working Drafts, as well as some of the issues that have been raised by the working group. As the Tracking Protection Working Group continues its process and completes its standards recommendations, we expect to have further refinements to this draft.

Executive summary/high-level comments

• The status quo is not normative; current tracking practices are anchored in business expectations of data flows that consumers generally would not like if they had full knowledge and understanding.
• Meeting user expectations should be the fundamental goal. We generally support Jonathan Mayer and Tom Lowenthal's approach to first- and third-parties.
• We agree that usability of DNT for users is critical. In general, DNT should operate as a "set it and forget it" mechanism. It is appropriate for websites to seek site-specific exemptions, but we would be concerned if such mechanisms were too daunting for users.
• The DNT standard must permit user-agents to ship with the default of DNT:1. We recognize that this is up to the user-agent vendor under the standard. DNT defaults and reset mechanisms should be obvious and transparent.
• We recognize that this standards process is consensus-based and should accommodate business interests to a reasonable extent.
• We welcome exchange of views and information regarding operational use and other exceptions/exemptions. This process has just begun, so we do not have many detailed comments about such exemptions. Our general approach will be to place the burden on business to explain and justify such exemptions. First, we wish to understand the business case. Given that the consumer/privacy groups are far from well informed about commercial practices, it will be important to unpack claims relating to security, fraud, etc. Second, we wish to understand whether there are good alternatives to current or proposed practices for which exemptions are sought. Mozilla's DNT field guide and other documents suggest that many operational uses can be accommodated under DNT with minimal cost to business. Third, if business interests cannot be so accommodated, we wish to understand why the business case should trump the user privacy interests at stake. The overall approach, we believe, will require detailed discussion about what data is actually needed for the particular purpose, how long it must be retained, and how it can be minimized while being useful.

1. Introduction

We appreciate the opportunity to participate as a Community Group in the W3C DNT process. We also appreciate all the work done by the W3C and working group members, especially the individual editors and drafters. This Community Group document represents the editors' best understanding of the CG members' views on the main issues presented to this date. We have ignored many of the more technical issues, and even for many of the policy issues our views remain unformed or unclear; when we do not address an issue, it does not mean that we agree with its current status. Nevertheless, this represents a good-faith effort to comment constructively on the WG work-product to date.

While the commercial Internet/digital media environment provides important forums for diversity of expression, communication, and information, it has been structured to collect nearly unlimited amounts of information on each user -- creating new forms of surveillance that raise crucial civil liberties and consumer protection concerns. In general, the user's interest in not being tracked must be recognized as a right to be respected, not an obstacle to be overcome in the pursuit of data collection.

Unfortunately, Internet tracking is invasive and pervasive. Wherever consumers go online and whatever they do is tracked usually without their knowledge and consent. What they click on, purchase, or share with others is compiled, analyzed and used to profile them. The data is often used to target advertising, but can also be used to make assumptions about people in connection with employment, housing, insurance, and financial services; for purposes of lawsuits against individuals; and for government surveillance.

In our view, the vast majority of what users do online is quintessential expressional behavior — reading, writing, speaking, and associating with others — protected under the Universal Declaration of Human Rights, Article 19, which provides the right to "seek, receive and impart information and ideas through any media and regardless of frontiers." In the United States, such activity enjoys significant constitutional protections against direct government interference (e.g., First Amendment law protects anonymous speech and privacy of association), but these protections can be circumvented when private actors keep records of online activity. Thus, for U.S. users, data about expressional activity is more weakly protected by law when it is stored by private actors.

Our concern here is therefore mainly about the practices and products of tracking and the data retained or derived from tracking. We recognize that businesses may have valid economic interests in tracking, but businesses must also recognize that users have valid privacy and civil liberties interests in not being tracked and in control of the data retained or derived from tracking if users consent to such tracking. Even if businesses have clear and uncontroversial legitimate purposes for tracking, civil litigants and government entities may be able to obtain access to data retained or derived from tracking for purposes inimical to users' interests.

Our view is that the status quo is a product of a particular technological regime that was not designed to protect user privacy, under which much information is available to websites simply by virtue of how user-agents work. While we take that status quo as a practical given, we do not regard it as normative. For instance, users did not agree that browsers should transmit HTTP referrer information, and we would welcome user control over whether such data should be transmitted. In other words, that businesses are accustomed to receiving information about users, user-agents or user devices does not mean that businesses are entitled to receive that information.

Given the status quo, citizens and consumers require tools, in addition to public policy, to protect their privacy. Existing tools are inadequate because they:

- **Don't actually work**: Opt-out often means you don't get targeted ads, but your information is still collected and your activities tracked.
- **Are too confusing**: Consumers don't have the expertise to choose what companies to block, or where to go to block them.
- **Require too many choices**: Ad companies, Web browsers, search companies, and Websites all have different privacy tools and consumers must act to protect themselves with each.
- **Don't make clear whom to trust**: There is no way for consumers to know if a privacy tool is a legitimate site, or if it is trying to trick them into giving up even more info (or worse yet, money!)

A "Do Not Track" mechanism is a method that allows a computer user to send a clear, unambiguous message that one's online activities should not be tracked. There are a number of ways this could be accomplished. In fact the "Do Not Track" concept is technology neutral. It is any method that sends the message to websites a consumer visits that one's activities should not be tracked. Simply put, "Do Not Track" is like posting a "No Trespassing" sign on your property. We leave to others the task of drawing the technical specifications for how such a message should be sent. At a minimum, however, the mechanism should be universal, easily usable, persistent, and cover all tracking technologies.

Tracking Preference Expression

Comments on Dec. 19 draft: http://www.w3.org/2011/tracking-protection/drafts/tracking-dnt.html

We begin with some very general comments about the document.

First, the introduction is written from the industry standpoint; e.g. the rationale for DNT is "we don't want to offend the user because this leads to lost revenue," rather than "the user has certain privacy rights that we must respect." Moreover, as noted above, users' privacy interests are aligned against both commercial and government actors.

Second, we are concerned about the presence of statements like "Advertising revenue is the single largest source of funding on the Web." We do not know if this is true and we question its relevance here. The Internet includes vast non-commercial contributions of universities, government, libraries, nonprofit organizations and individual users. We expect that the W3C DNT standard will be adopted by these non-commercial entities as well.

Third, the document frequently uses the term "cross-site tracking," and we think it should simply refer to "tracking."

ISSUE-2: What is the meaning of DNT (Do Not Track) header?

The document states:

[CLOSED] "Does the presence of a DNT header field on requests always indicate an explicit choice." The answer we agreed upon is "yes."

As noted earlier, we do not wish to prevent user-agent vendors from shipping with a default of DNT: 1, and we have some concern that the current language may do so. We believe that the current statement of ISSUE-4 permits user-agents to ship with DNT enabled. We equally believe that user-agents should not ship with a default of DNT:0.

ISSUE-40: Enable Do Not Track just for a session, rather than being stored

The document states:

[CLOSED] Resolved in DNT Call 2011-10-26: The user agents are free to send different DNT values for different sessions. We agreed that this is a user-interface issue and out of scope on its own.

ISSUE-70: Does a past HTTP request with DNT set affect future HTTP requests? No

These issues appear related. We strongly prefer that DNT settings persist across sessions until modified by the user. We do not object to the standard's permissiveness here as a technical matter—when the DNT header is sent, servers need not "remember" previous sessions—but DNT will be significantly more valuable to users, and will better meet users' expectations, if DNT need not reset each time users visit a website. A non-normative reference about the value of persistence may be appropriate here.

Other closed issues

We agree with the following:

ISSUE-50: Are DNT headers sent to first parties? Yes

ISSUE-68: Should there be functionality for syncing preferences about tracking across different browsers?

[CLOSED] Resolved in DNT Call 2011-10-26: The user agents may or may not sync. However, this is out of scope for this spec.

ISSUE-42: Feedback to the user from the browser when Do Not Track is turned on: Yes, consistent with the apparent consensus on ISSUE-81.

Other major issues

We understand the basic DNT configuration to have 3 possible states:
• DNT:1 (enabled, header sent)
• DNT:0 (enabled, header sent)
• Silence (user-agent lacks any DNT capability, or user/intermediary/user-agent did not set DNT (no header sent))

ISSUE-13: What are the requirements for DNT on apps/native software in addition to browsers?

We agree that W3C should use “the term *user agent* to refer to any of the various client programs capable of initiating HTTP requests, including browsers, spiders (web-based robots), command-line tools, native applications, and mobile apps.”

One comment: the specific reference to HTTP may not be sufficiently technology-agnostic. For instance, the SPDY protocol may become more popular, and while current SPDY clients probably are “capable of initiating HTTP requests,” we do not know whether future clients might lack that capability. Nor would we want entities to end-run DNT by using protocols like ftp.

ISSUE-4: What is the default for DNT in client configuration (opt-in or opt-out)?

Our understanding is that the current consensus is agnostic, leaving it up to user-agent, so a browser MAY ship with DNT enabled [“We do not specify how that preference is configured: the user agent is responsible for determining the user experience by which this preference is set.]. This is acceptable for the technical standard, although we clearly prefer that DNT be set to “1” by default based on the belief that users generally prefer not to be tracked.

ISSUE-95: May an institution or network provider set a tracking preference for a user?

[current language] “An HTTP intermediary *must not* add, delete, or modify the DNT header field in requests forwarded through that intermediary unless that intermediary has been specifically installed or configured to do so by the user making the requests. For example, an Internet Service Provider must not inject DNT: 1 on behalf of all of their users who have not selected a choice.” Our understanding is that there is no strong consensus here. We agree with the flat prohibition on intermediary modification of a user’s choice. We also prefer omitting the second paragraph about "There are some situations where an entity wishes to express a Do Not Track preference on the user's behalf.” There is some interest in permitting intermediaries, when the user made no DNT choice, to set DNT: 1 (but not DNT: 0). This is a minority view provided for completeness’ sake.

ISSUE-78: What is the difference between absence of DNT header and DNT = 0?

“[PENDING REVIEW] Proposed text above defines that a "0" may only be sent when DNT is enabled and some mechanism known to the user agent has specifically made an exception for this origin server. Note that we have not defined such a mechanism (and probably won't do so). If DNT is disabled or not implemented, no DNT header field is sent. In the absence of regulatory, legal, or other requirements, servers are free to interpret the lack of a DNT header as they find most appropriate for the given user, particularly when considered in light of the user's privacy expectations and cultural circumstances.”

We agree that DNT silence is merely silence as a technical standard. In light of ISSUE-98: Consider applicable laws and regulations, such as Article 5(3) of the EU ePrivacy Directive, our understanding is that DNT silence will have concrete meaning in the EU, Canada, and any jurisdiction where the legal regime has more stringent consent rules than the United States. We discuss this further in the context of ISSUE-8, below.

ISSUE-81: Do we need a response at all from servers?

"[PENDING REVIEW] Yes: The users expect to be able to see whether a DNT header is accepted, rejected, or sent into the void."

We agree, server response is critical and lack of response should mean noncompliance with the standard.

ISSUE-79: Should a server respond if a user sent DNT:0?

Yes.

ISSUE-51: Should 1st party have any response to DNT signal?

Yes, all parties should acknowledge receipt of DNT header. No response signals noncompliance. First parties have definite DNT obligations. We emphasize again that while we generally accept the first-/third-party distinction as articulated by Mayer and Lowenthal for purposes of W3C's DNT process, many of us would like to control first-party tracking as well (but recognize that consensus would not be likely on this point).

Our acceptance of the Mayer-Lowenthal approach turns partly on its careful refusal to permit tracking by commonly branded affiliates under DNT: 1. Commonly branded affiliates may be in very different types of businesses and the fact that they share a corporate name is no guarantee that consumers will understand who they are or what they might do with their information.

ISSUE-105: Response header without request header?

If DNT=1, site MUST send response header (for compliance validation) (if no response header sent, this would mean non-compliance with spec)
If DNT=0, site MUST send response header (Issue-79)
If no DNT header at all, site MAY send response header

We agree here.

5.6 Status code for Tracking Required: An HTTP error response status code might be useful for indicating that the site refuses service unless the user either logs into a subscription account or agrees to an exception to DNT for this site and its contracted third-party sites.

We agree.

ISSUE-46: Enable users to do more granular blocking based on whether the site responds honoring Do Not Track

We are not entirely sure what this issue means. If the site honors DNT, doesn't that mean that it complies with the DNT header received? We support more granularity that gives the user more usable control, perhaps over tracking otherwise permitted under DNT: 1; sites that honor DNT may wish to be more privacy-protective. We have some concern that too much granularity can make DNT unwieldy and less attractive to users.

ISSUE-43: Sites should be able to let the user know their options when they arrive with Do Not Track

We generally agree. There is some concern that sites will simply say "if we can't track you, you can't use the site," while others of us also believe that this will be unlikely. We are curious about the working group's sense here.

ISSUE-47: Should the response from the server point to a URI of a policy (or an existing protocol) rather than a single bit in the protocol?

A possible danger here could be that the response points to a site privacy policy that tries to circumvent the user's expressed DNT preference. We believe that such behavior would be non-compliant with the standard.

ISSUE-87: Should there be an option for the server to respond with "I don't know what my policy is"

No. If the site represents itself as DNT-compliant, it must know its policy. If it does not know its policy, it is not DNT-compliant.

Tracking Compliance and Scope

Comments on Dec. 14 draft: http://www.w3.org/2011/tracking-protection/drafts/tracking-compliance.html

ISSUE-8: user knowledge/expectations

Instead of the technology, we focus on websites' compliance with a DNT request and user expectations when they opt to send the DNT message. The question of user expectations is a persistent theme in ongoing W3C discussion of DNT. We are greatly concerned that many stakeholders cannot put themselves in the ordinary web user's place, expect users to understand more of what is happening on the web than they actually do, and accordingly impute more consent or even acquiescence of existing tracking practices than is realistic.

Furthermore, even if users were as well informed as many stakeholders seem to think they are, users currently lack the tools to make their desires known. Indeed, the idea of DNT has become popular partly because businesses have deliberately circumvented users' attempts to express their rejection of tracking. For example, when methods were developed to block tracking "cookies," trackers got around that by using flash cookies.

We also focus, where appropriate, on legal regimes that establish different user expectations as a matter of public policy. For instance, while the United States does not have a general background consumer privacy law that clearly resolves consent issues, other legal regimes do.

Canadian opt-out approach

Under the recent Canadian guidance,

“Any collection or use of an individual’s web browsing activity must be done with that person’s knowledge and consent. Therefore, if an individual is not able to decline the tracking and targeting using an opt-out mechanism because there is no viable possibility for them to exert control over the technology used, or if doing so renders a service unusable, then organizations should not be employing that type of technology for online behavioral advertising purposes.”

Furthermore,

“Opt-out consent for online behavioral advertising could be considered reasonable providing that:
“• Individuals are made aware of the purposes for the practice in a manner that is clear and understandable – the purposes must be made obvious and cannot be buried in a privacy policy. Organizations should be transparent about their practices and consider how to effectively inform individuals of their online behavioral advertising practices, by using a variety of communication methods, such as online banners, layered approaches, and interactive tools;
“• Individuals are informed of these purposes at or before the time of collection and provided with information about the various parties involved in online behavioral advertising;
“• Individuals are able to easily opt-out of the practice - ideally at or before the time the information is collected;
“• The opt-out takes effect immediately and is persistent;
“• The information collected and used is limited, to the extent practicable, to non-sensitive information (avoiding sensitive information such as medical or health information); and
“• Information collected and used is destroyed as soon as possible or effectively de-identified.”

As we read this guidance, DNT silence would generally not permit tracking, and websites would need to implement other mechanisms in order to track in Canada. Conversely, it would seem that compliance with DNT would go a long way toward satisfying Canadian consent requirements, assuming that the user agent is DNT-capable in the first place.

EU/Art. 29 Working Group approach

The European Union may take a stronger position on consent. As we read the recent Article 29 Working Group opinion on behavioral advertising (Opinion 16/2011), a DNT mechanism may be permissible under the e-Privacy Directive so long as “no tracking” is the default.

Under EU principles, prior explicit opt-in consent is necessary for lawful tracking, and notice must be provided to users before data processing occurs. The Article 29 Working Group takes the position that such notice must include at least the following elements: who (which entities) collect data; what data is collected; that “profiles” (derived data, summaries, inferences, etc.) are created, and for what purpose or purposes; that the collection enables user identification across multiple websites; the duration of data or profile retention; the duration of any user informed consent.

The Article 29 Working Group focused mainly on cookie-based tracking, but suggested that a DNT mechanism could satisfy its requirements so long as the default state was “no tracking.”

This has implications for W3C, in that the current consensus is agnostic as to browser defaults. We have three distinct user expressions: user rejects tracking; user accepts tracking; user is silent (does not make a DNT choice). The W3C consensus appears to be that when the user is silent, websites have no compliance duties. Under the EU opt-in regime, it seems that user silence equals a user's rejecting tracking. Under the Canadian regime, it seems that user silence could permit tracking, but only if the browser actually included a qualifying DNT mechanism or if the website had its own qualifying mechanism. If neither is present, then silence would not permit tracking ("if an individual is not able to decline the tracking and targeting using an opt-out mechanism because there is no viable possibility for them to exert control over the technology used, or if doing so renders a service unusable, then organizations should not be employing that type of technology for online behavioral advertising purposes.").

2. Scope and goals

For purposes of these comments, we treat all of the data at issue as personal and identifiable data, because this data is at least initially associated with the user's device, whether by IP address, a MAC address, or some other identifier (IMEI, IMSI, etc.). Even if users share devices, we believe that in a significant proportion of cases the device linkage is meaningful to the data collector (e.g., as expressing the purchasing preferences of a household as a unit), or that data collectors can disaggregate shared use (e.g., distinguishing between child and adult users in a household by destination, time of day, etc.). We will address proposals for de-personalizing data (aggregation, de-identification) as they emerge.

3. Definitions

First and third parties[1]

Various issues (10, 26, 49) are about the meaning of the first-party/third-party distinction. We generally agree with the Mayer-Lowenthal approach here, with minor points articulated below. We believe agree that the key principle underlying this distinction is consumer expectations, and not technical concerns such as domains or same-origin, as stated by Roy Fielding. Branding is relevant as a factor in consumer expectations, but not as an independent principle or test.

When a user enters a URL and visits a specific website, that site which has its address in the user's browser address box is considered the First Party site. By convention the user is the Second Party and all other sites are Third Parties. Because a user is directly interacting with the First Party there is an implicit understanding that data will be shared with the site. There is,

[1] Chris Calabrese likes the Rush HR 5777 def'n (10) THIRD PARTY-

(A) IN GENERAL- The term 'third party' means, with respect to any covered entity, a person that--

(i) is not related to the covered entity by common ownership or corporate control; or (ii) is a business unit or corporate entity that holds itself out to the public as separate from the covered entity, such that an individual acting reasonably under the circumstances would not expect it to be related to the covered entity or to have access to covered information the individual provides to that covered entity.

however, no user expectation that data will be shared with unknown Third Party sites. The reality, as the Wall Street Journal's "What They Know" series pointed out, is that Third Party tracking is extensive. The nation's 50 top Websites install an average of 64 pieces of tracking technology on users' browsers – all without your knowledge. This tracks all of your activity online, adds it to your profile, and then puts it up for instant sale in a stock market-like auction. And while the First Party/Third Party distinction is a useful analytic tool in assessing user expectations about Do Not Track obligations, it is also true that the distinctions between First and Third Parties are eroding, as the role of ad exchanges and demand side platforms, illustrate.

Hidden webpage elements are, of course, core cases of third parties. They are deliberately concealed from users, and the average user is unaware of: web bugs or beacons; tools that can reveal them; how to prevent such elements from tracking them. Visible, conspicuous webpage elements like ads and widgets must also be treated as third parties. The average user does not realize that many ads are served by third parties rather than the first-party website they are visiting, or that information about the user is transmitted to those third parties. We believe that there is a general consensus on this point—that all of these webpage elements are third parties for DNT purposes.

ISSUE-26: Providing data to 3rd-party widgets -- does that imply consent? Our general answer is no. That said, Jonathan Mayer's formulation — "A 'first party' is any party, in a specific network interaction, that can infer with high probability that the user knowingly and intentionally communicated with it. Otherwise, a party is a third party."—may be sufficient. Our discussion below is tentative given the range of views within the Community Group.

We also detect a weaker consensus on the general idea that a visible third party can become a first party for DNT purposes if and only if the user engages in "meaningful interaction" with the window or widget. We do not entirely agree here.

First, stipulating for W3C purposes that users "expect" tracking by the sites they visit (in general, large well-established venues), it is not clear that users expect such recording tracking from widgets at all. Many widgets appear as an app that simply performs a specific function. In the case of a weather, stock or map widget, it may simply return a result, and the user may perceive the widget as merely an application without any memory. Indeed, we know that several years ago, many consumers thought of Google Search in this way and were surprised to learn that Google retained search histories.

Second, even if users expect a widget to record data about them, they may not understand that a commonly branded widget is part of a hive mind. Branding and sharing data aren't the same thing. As Jonathan Mayer stated,

"Example 1: The user visits a site with a clearly-branded Accuweather.com weather widget. The user recognizes the branding and scrolls the widget forward to see tomorrow's weather. The user expects to simply move the forecast ahead; the user does not expect Accuweather to collect cross-site tracking data."

That understanding could be different for well-known social widgets, such as from Facebook, Google, Twitter, etc. Our point is that an expectation of tracking by the widget is not the same as an expectation of the data's being sent anywhere else.

Part of this may be the nature of the interaction. Some third parties may behave in ways that make things much clearer. Maybe if you click on the Chips Ahoy ad you go to the Nabisco site or get Nabisco content, and it could be fair to say that Nabisco has become a first party. But it cannot be said categorically that deliberately clicking on a widget or other third-party element automatically confers first-party status. Put another way, an unknown party should not be endowed with first-party status merely because the user knows that party differs from the main page yet interacts anyway.

ISSUE-49: Third party as first party - is a third party that collects data on behalf of the first party treated the same way as the first party?

Here again, we agree with the Mayer-Lowenthal approach, which we understand to restrict third parties. An overly permissive approach to third parties acting on behalf of first parties would negate DNT's value. In the outsourcing of analytics example, it is critical that the third-party analytics provider silo all data collected on behalf of a first party and not make it available in any way to any entity other than that first party. Indeed, such siloing should be enforced technically per the ISSUE 73 draft.

ISSUE-5: What is the definition of tracking?

Current text: "Behavioral tracking is the collection and retention of transactional data about the web-based activities of a particular user, computer, or device across non-commonly branded entities in a form that allows activities across non-commonly branded entities to be attributed to a particular user, computer, or device, over time, for any purpose other than the explicitly-excepted purposes specified below."

We dislike this definition for several reasons. First, issues related to party status (branding), identifiability, purposes, exceptions, etc. need not be resolved in the definition of tracking. Second, we do not see the need to limit the definition to "behavioral," "transactional data" or "particular" users or devices etc. For instance, the current definition of "transactional data" refers to "information about the user's interactions with various websites, services, or widgets which could be used to create a record of a user's system information, online communications, transactions and other activities, including websites visited, pages and ads viewed, purchases made, etc." We worry that building many restrictions into the basic definition will create unnecessary ambiguity and may inadvertently exclude relevant data.

It seems much simpler to use a broad definition, e.g. "Tracking is the collection of data about Internet activities of a user, computer, or device (including mobile phones and devices), over time and across a Website or Websites."

Specific enumerated purposes, such as site maintenance and improvement, fraud prevention or legal compliance may warrant exemptions if they are well defined. [note Art. 29 point that the exemption would be limited to certain requirements e.g. prior notice and consent, without exempting from minimum necessary, revocation, spoliation etc.]

We do not limit our understanding of tracking from a policy or rights perspective to cross-site tracking. As explained earlier, our concern about tracking stems ultimately from the retention of data about users' online activities, and the fact that such data is maintained by first-party websites does not prevent other parties (such as the government) from obtaining that data and correlating it across multiple websites.

We nevertheless agree that in the W3C DNT context, it may be possible, and will be valuable, to develop a consensus around the mechanisms for addressing cross-site and third-party tracking. Our point here is that we are also concerned about first-party tracking, even if W3C DNT does not address it.

ISSUE-16: What does it mean to collect data? (caching, logging, storage, retention, accumulation, profile etc.)

We believe that ALL of these should be included within "collect data," but accommodations can be made for specific contexts. We expect that the WG will address minimization techniques, e.g. de-identification, truncation, and real-time or near-real-time deletion (ephemeral storage),

ISSUE-92: If data collection (even very specific with IP address, user agent, referrer) is time-limited, with very limited retention, is that still tracking?

Yes. Given the technical status quo, passive collection of protocol information will happen, but we see no reason to define such passive collection out of the definition of tracking. The preferred approach would be to create specific, well-justified exemptions with appropriately tailored minimization or other safeguards.

ISSUE-89: Does DNT mean at a high level: (a) no customization, users are seen for the first time, every time. (b) DNT is about data moving between sites.

We are not sure what this issue is really about.

ISSUE-97: Re-direction, shortened URLs, click analytics -- what kind of tracking is this?

We believe that all of these are third-party tracking. We agree with Justin Brookman's email comment:

"I can't think of a single URL shortener scenario that looks like a first-party interaction. If I read this on Twitter: "Neat WSJ story on #privacy in the cloud: goo.gl/eT3d" and click on the link, I think the WSJ is the first party and Google is a third party. I'm clearly not trying to interact with Google – someone just used that service to get under 140 characters, and I could care less whether they used bit.ly, j.mp, t.co, c.dt or anything else."

We recognize that we may not understand all of the corner cases here, but in general it seems that the user does not intend to interact with the third party.

ISSUE-55: What is relationship between behavioral advertising and tracking, subset, different items?

Behavioral advertising uses tracking to create a profile of the user and then serve targeted ads. Many industry privacy "solutions" only stop the serving of ads — but not the tracking, which is our focus. When DNT is enabled, the site must not track (with the exception of specified exceptions).

ISSUE-71: Does DNT also affect past collection or use of past collection of info?

Yes.

Other issues

ISSUE-36: Should DNT opt-outs distinguish between behavioral targeting and other personalization?

No, but we welcome further elaboration. In general we see no need for a distinction. Our underlying focus is on the tracking, so the real issue is whether the personalization uses tracking. We agree with the draft that "when the header is set to DNT:1, then this will indicate that no personalization should occur," and that previously collected data would not be used.

We are uncomfortable with the exceptions in the draft specification. For instance, we disagree with the example: "An individual visiting a news site will expect to see local news and weather based on her current location regardless of DNT header setting." Such person may expect news and weather based on her home location even when traveling abroad. The general exception for "When it is individual's expectation that personalization will occur" seems too elastic in the face of DNT: 1.

Also, the exceptions in the draft specification touch on several different issues that may need to be resolved first: treatment of the collection-retention distinction; geolocation data; and the interaction of DNT with other user-configured settings, including logging status.

Issue-30: offline data

The issue seems to be: "Should we address the association of first party data with third party data? What does this standard say about a first party associating offline data from a third party with their own data and then using that in targeting? How about the first party associating it with third party data and/or selling it to a third party?"

We believe that DNT: 1 means no transfer of data and no use of offline data.

--first parties MUST not offline transfer any data to any third parties that they could not online transfer to

--first parties MUST not offline transfer any data to any parties not subject to DNT (because that could easily circumvent DNT)

--third parties MUST not offline receive any data from any parties subject to DNT that they could not online receive

We believe that “offline append” is included. Users don't want to go to a first-party site and see "We saw that you bought adult diapers when you last went shopping! Want to buy some more?" At that point, it has become online data even if it didn't start that way, and seems to be fully in scope.

Issue-32: Sharing of data between entities via cookie syncing/identity brokering

We do not fully understand the current draft, but we fear that it could undermine DNT. It may also be insufficiently technology-agnostic. We welcome further elaboration.

4. Compliance with an expressed tracking preference

First-party compliance with DNT message

We believe that when a First Party receives a DNT message:

The First Party MUST NOT share users’ data with third parties. An exception would be if the Third Party is acting as an agent performing a function only for the First Party and does nothing else with the data. An example might be analytics. If the Third Party is the agent of multiple First Parties, it must silo each First Party’s data without any sharing or analysis across data silos.

The First Party SHOULD collect only the data necessary to complete the transaction during the current session and not store the data over time, without the users’ explicit informed consent.

ISSUE-17: Data use by 1st Party (overlap issue)

As stated above, it would be preferable if first parties did not track if DNT: 1 (should not).

ISSUE-54: Can first party provide targeting based on registration information even while sending DNT

No. As we understand the issue, this is about first parties sending data to others in the face of DNT: 1.

ISSUE-59: Should the first party be informed about whether the user has sent a DNT header to third parties on their site?

Yes.

ISSUE-91: Might want prohibitions on first parties re-selling data to get around the intent of DNT (overlap issue)

Yes.

Third party compliance

When a Third Party receives a DNT message, it MUST NOT collect data from a user without the users’ explicit informed consent.

When a Third Party widget is embedded in a First Party site, is clearly branded and the user has meaningful interaction with the widget, it becomes a First Party site for the transaction and it

MAY collect data necessary for the transaction. It MUST NOT retain the data beyond the session.

ISSUE-39: Tracking of geographic data (however it's determined, or used)

Current draft text: “This specification does not place limitations on the use of geolocation technologies by the operators of third-party domains.”

We disagree. There has been significant public concern about geolocation in various contexts recently. DNT=1 should block all third-party geolocation, because users who express the no-tracking preference probably object to geolocation, subject to valid exemptions. ISSUE-36 touches on this issue, generally in a reasonable way, but we don’t see why IP-based reverse-lookup geolocation should be automatically permitted. In any case, we believe that users want to be able to express the preference about geolocation, and it is reasonable for DNT: 1 to be used for that purpose.

Exemptions generally

Our comments here are fairly abstract. As stated at the outset of this document, our general approach will be to place the burden on business to explain and justify such exemptions concretely. There are certainly important business interests here, but these must be clearly specified. At this time, we have had very little detailed discussion, and we have not reviewed all of the extant drafts.

Transparency is especially important here, because these exemptions permit tracking even in the face of DNT: 1. The standard should require websites to inform users about their practices with respect to these exemptions.

ISSUE-22: Still have "operational use" of data (auditing of where ads are shown, impression tracking, etc.)

The current draft describes operational uses. We need to better understand what data is needed, for which operational uses, for how long, etc. We also need to account for the existence of ways of accommodating business interests under DNT.

Issue-31: Minimization for exemptions -- to what extent will minimization be required for use of a particular exemption? (conditional exemptions)

Here, we believe an issue-by-issue approach is needed. For example, Mayer’s IETF DNT draft stated that “Protocol logs used solely for advertising fraud detection, and subject to a one month retention period” and “Protocol logs used solely for security purposes such as intrusion detection and forensics, and subject to a six month retention period.” We do not accept these specific minimization proposals, because we lack good data about why these retention periods were chosen, but the general approach seems reasonable.

ISSUE-23: Possible exemption for analytics, ISSUE-34: Possible exemption for aggregate analytics

We have not reviewed this draft yet.

ISSUE-73: In order for analytics or other contracting to count as first-party: by contract, by technical silo, both silo and contract

We have not reviewed this draft yet, but generally agree that both technical silo and contract should be used.

ISSUE-24: Possible exemption for fraud detection and defense

We recognize that fraud detection and defense is a significant interest, but there has been insufficient discussion of the details for us to comment further.

ISSUE-25: Possible exemption for research purposes, ISSUE-74: Are surveys out of scope?

We believe that surveys are in scope. More discussion is needed on the meaning of "research."

ISSUE-28: Exception for mandatory legal process

This is unavoidable, but the standard could benefit users by increasing transparency. For instance, Google has been a pioneer in informing the public about its responses to surveillance requests. Some U.S. service providers routinely notify users/subscribers about subpoenas, when legally permitted to do so. Where the law itself is unsettled about the legal process required to compel production or collection of data, companies can be more transparent about what they insist upon — in the U.S. context, for instance, companies may have policies about whether they always require a warrant for some kinds of data.

ISSUE-75: How do companies claim exemptions and is that technical or not?

[transparency again? In privacy policy/TOS?]

Issue-15: what special treatment for children's data?

Current draft specification: "The DNT: 1 header does not require special treatment for children because DNT:1 means no tracking regardless of whether the user is a child or not. Note that operator handling of children's data may also be governed by local laws and regulations, such as COPPA in US."

We generally agree, but there is strong dissent within our group that would treat websites aimed at children differently.

5. User Interactions

We are still discussing this section.

6. Interaction with other tools

We are still discussing this section.
###