Working Draft: This is our effort to compile the previous discussions and proposed text with regard to use of first party data in a third party context within the Tracking Protection Working Group. We apologize for any missed text or viewpoints or for including any unrelated issues.

First Party Data in Third Party Context (including Append discussion)

Note: The March 31, 2013 text and comments of April 8, 2013 about append are in this document at the end.

Tracking Compliance and Scope March 6, 2013

http://www.w3.org/2011/tracking-protection/drafts/tracking-compliance.html#first-party-data

6.1.1.2.3 Content or Ad Delivery Based on First Party Data

Option

Information may be collected, retained and used for the display of content or advertisements based in part on data that the third party previously collected from the user when acting as a first party.

Note

This text may be revised to offer two alternatives: first parties can use any data to offer content in the third party context, or first parties can only use declared data to offer content in the third party context. Shane Wiley has proposed defining "declared data" as information directly and expressly supplied by a user to a party through meaningful interaction with that party.

The issue is also contingent upon what identifiers third parties can use when Do Not Track is turned on. If third parties cannot read cookies, they may be unable to associate first parties in third-party scenarios.

Others have argued that this language is unnecessary because the standard places no limitations on the use of first party data.

Tracking Compliance and Scope Oct. 2, 2012

http://www.w3.org/TR/tracking-compliance/#first-party-data

6.1.1.3 Content or Ad Delivery Based on First Party Data

Note

Note that it is not clear that this is in scope, per Shane; others disagree. Revisit whether contextual belongs in some place other than permitted uses (potentially the definition of collection).

Option

Regardless of DNT signal, information may be collected, retained and used for the display of content or advertisements based in part of data that the third party previously collected from the user when acting as a first party.

6.1.1.3.1 Examples

This section is non-normative.

1. A user visits ExampleNews.com with DNT:1 enabled to read a story about a national election. ExamplesNews uses the third party ExamplePortal to serve content and advertisements on its site. ExamplePortal is not an outsourcing partner of ExampleNews. The user had previously visited ExamplePortal.com with DNT:1 enabled and read several stories about golf. ExamplePortal may serve an advertisement related to golf to that same user on ExampleNews. However, ExamplePortal may not use the fact that user went to ExampleNews to add to the user's ExamplePortal profile, and may only retain and use information about that fact for a permitted operational use.
2. A user visits Example Music with DNT:1 enabled to listen to recently released albums streamed online. Example Music uses the third party Example Social to provide a widget that shows users what their Example Social friends have done on ExampleMusic. ExampleSocial is not an outsourcing partner of ExampleMusic. The user is a member of ExampleSocial and has several friends who also share information about what they do on ExampleMusic on ExampleSocial. ExampleSocial may display information that the users' friends had shared on ExampleSocial related to ExampleMusic within its third-party widget on ExampleMusic. However, ExampleSocial may not use the fact that user went to ExampleMusic to add to the user's ExampleSocial profile, and may only retain and use information about that fact for a permitted operational use.

Discussions and proposed text ordered from earliest to latest:

Discussion started Feb. 5, 2012:

S Harvey:

- "Can first parties customize their own websites or advertising based on their own user data when a DNT header is ON?"

Shane Wiley:

- And the proposed answer, "YES", as this appears to capture the 1st party exception cleanly and we have other statements that disallow a 1st party from sharing information with 3rd parties when DNT:1.

David Wainberg:

- Also, going back again to the notion of cross-site data, if the data is cross-site, then it should be clear the party can't use it. So this question is another way of saying, "When DNT header is on, can first parties customize their own websites or advertising based on non-cross site data collected about their users? And the answer should be 'yes'. Do we need to clarify what "their own user data" is?

JC Cannon:

- I agree that first parties can customize their own websites or advertising based on non-cross site data collected about their users. There should be some transparency to users about this practice, but I feel it is out of scope to include in the standard.

Justin Brookman:

- I think Sean's restatement of the issue is a bit ambiguous. The key question is not whether a first party can alter its own websites and advertising on those sites based on data it collected as a first party. It's about whether they can then leverage that data when they're in a third-party environment.
- I was tasked with writing up language on this in Brussels, but upon reflection, my vision is already allowed for in the text: a third-party may customize content or advertising on other sites

based on data it had collected as a first-party. Thus, Yahoo! can serve ads on the New York Times based on what I had done on the Yahoo! site (or registration information I had provided to Yahoo!) and Facebook can tell me what my friends like in a social widget when I go to the WashingtonPost.com --- as long as neither collects the fact that I went to NYT or WaPo (apart from exceptions like ad reporting, fraud, analytics) and certainly does not add that information to a profile about me. The language in the draft currently allows for this. However, I will try to put together some non-normative language on this today to make it clear. I have heard the argument that this unduly favors first-party sites who have a lot of user data, but I also think the privacy implications are dramatically reduced when ads are influenced based on data that a party already has about you.

- Shane, you had seemed to disagree with this idea in Brussels, so if you want to put forward a countersuggestion that's fine. Alternatively, Tom had disagreed on one of the calls that Facebook should be allowed to personalize content based on data it had collected as a first-party, so he may want to proffer another suggestion. I could see a stronger argument against allowing Yahoo! to use passively-collected data about what I read on the Yahoo! site rather than using affirmatively provided info, but I personally wouldn't draw the line there. It's also possible this issue is currently being discussed elsewhere on the mailing list, but I have not remotely been able to keep up.

Jonathan Mayer:

- In the interest of clarity, I recommend we make two ISSUEs from ISSUE-54.
    - 1) What can a first party do on its own website with provided information? I completely agree with Shane that this falls into the current first party proposal, and I expect we'll get consensus and close the ISSUE quickly.
    - 2) What can a first party do with submitted information when it's a third party? We've already heard a range of views on this; I expect lengthy discussion and perspectives from many stakeholders before we close the ISSUE.

Jeff Chester

- I don't think if DNT is enabled a third party should be able to engage in profile-based targeting that they have collected as first party, as Justin perhaps as proposed. That would weaken user intent on DNT.

John Simpson

- I agree that when a site acts as a third party it MUST not engage in targeting based on data gathered when it was a 1st party if DNT is enabled.

JC Cannon

- I would like to drill into this a little further. How would this apply to a logged in state? If I'm logged into a social site and reading an article I would be interested to know if people I trust from that social site enjoyed the article or not without necessarily letting people know that I viewed the article, unless I select the share button. I don't want to have to enable tracking just to see if my friends liked the article.

Jeff Chester

- DNT:1 serves as a form of granular privacy protection. If one has DNT:1 on, they don't want tracking process working--even if it means they can't find out their friends enjoyed reading your latest book! Happy to discuss.

JC Cannon

- I disagree with your position, because I would still want that feature if I'm logged in and have DNT:1 enabled. This is part of the concern I have about making decisions for consumers that they may not want. If I can disable the article annotation by logging off from the social site, why bundle it with DNT taking away my flexibility?

John Simpson

- My first analysis is that if you're logged in to the service, you're having a meaningful relationship with it. That would imply they are a 1st party and can treat you accordingly. If you're not logged in, the social site MUST NOT use information that it has gathered while it had a first party relationship with you.

Jonathan Mayer

- I've seen a few suggestions that I'd disagree with on this thread. Since they seem fairly independent, I'll break them out individually.
    - 1) We should allow social widget personalization because some users might want it.
        - The same argument applies to any prohibited practice. That's why the TPE specification provides an explicit exception mechanism. If a user wants to see more personalized content from a third party or using third-party data, whether stuff their friends liked or (tracking-based) interest-targeted advertising, they can provide an exception. We mocked up an exception flow for Facebook's social widgets at http://donottrack.us/cookbook/.
    - 2) Social widget providers are first parties if the user has logged in since the user has a business relationship with the website.
        - I thought we had agreement in Santa Clara and on the list that third-party widgets become first party by means of user interaction, not logged-in status.
    - 3) Social personalization isn't the same as third-party data collection.
        - I don't follow this line at all. Embedded social content is from a third party, and that third party collects data. Moreover, the data collection practices currently used for social personalization rely not only on a unique ID—they rely on an ID tied to the user's identity.

JC Cannon Proposal

- How about this:
    - 1) For social sites, manage social feature at that site or by logging out.
    - 2) For tracking and personalization opt-out use DNT.

Shane Wiley

- Wouldn't the current Facebook structure be considered an "out of band consent" exception? Meaning the user has already given FB consent to this data collection web wide?

Jonathan Mayer

- This is why standards of notice are important. If "the user has already given Facebook consent" means Facebook asked explicitly for permission to identify the user on other sites and got an exception through the exception API, all's well. But if Facebook merely links to its privacy policy at signup, no, that's not enough notice. To the extent others believe it is, I'd like to hear why social networks deserve a special carve out from the ordinary rules.

- That's all, however, independent of the issue you raised: does Do Not Track impose limits on third parties when 1) the user has an account, and 2) the user is logged in? I think the answer should be yes - the very same limits it imposes on any other third party.

Chris Pedigo

- As for this specific issue, we believe that a DNT standard should be about giving consumers the ability to opt out of tracking by parties with which they have no relationship. But, clearly in this case, consumers do have a relationship with the entity where they set up an account. And, FWIW, setting up an account with an entity is just about the highest level of consent that a consumer can give. Even the most uneducated web surfers (i.e. my parents) would never set up an account with an entity that they didn't know and trust to a certain extent. On top of that, they have a very effective option of simply logging out. Many consumers want the ability to share content with their friends and family. JC is correct....if a DNT standard complicates their ability to easily share content then users are more likely to be frustrated with the DNT standard.

David Singer

- I am saying that there are two scenarios already covered by our specs, for a user using DNT:
  - a) they do NOT opt-in to this site that is sometimes 1st, sometimes 3rd; under those circumstances, the widget shown in 3rd party status is the same as the one shown to unknown people
  - b) they DO opt-in, possibly in-band, possibly out-of-band; then the 3rd can show personalized content.
- Given the existence of an opt-in, to achieve case (b), we don't need to bend case (a) to behave the same as (b). Case (a) can and should stay in the "treat me as someone about whom you know nothing and remember nothing" camp. IMHO. I think.

Agenda March 21, 2012 Call

- 9. ISSUE-54: Can first party provide targeting based on registration information even while sending DNT?
- We have a suggestion of no text from Justin, some discussion on the mailing list that meandered around many other topics, and then we were caught up in the next publication. Let's see if we can move to a more productive conversation by phone. It is possible that this issue will resolve itself easily based on how other issues work out -- if we're still going in circles after a little while, I'll suggest we close the actions against it (action-68, action-69, action-109) and postpone for now.

Declared Data:

Amsterdam Face to Face Oct. 4

- *WileyS:* terms we use are 'observed data' and 'declared data', think that's the distinction, and we agree on observed and are discussing declared
- <*justin*> In the current text, usage is not limited to declared data. I would happy to revise, however.
- *WileyS:* rejoices at the agreement, but takes an action to define declared data
- *amyC:* want to check where we are going. does DNT even govern declared data at all, as opposed to observed? it might lead to bizarre scenarios ('do you really want to fill in this survey? you have DNT on!')

- *aleecia:* the text currently covers both declared and obsered and allows use (it may be imprudent)
- *achapell:* take a hypothetical: can Apple take an iTunes playlist and set up an ad network and use that data for targetting?
- *achapell:* take a hypothetical: can Apple take an iTunes playlist and set up an ad network and use that data for targetting?
- *dwainberg:* echo Alan's concerns. also some questions
- <*trackbot*> Created ISSUE-179 - Make sure in the spec that we clarify information provided explicitly by a user (e.g. data typed into a form on a site with a clear privacy policy) is not subject to DNT. ; please complete additional details at http://www.w3.org/2011/tracking-protection/track/issues/179/edit .

Declared data discussion started October 16, 2012:

Shane Wiley Proposed text

- Proposed text per our discussions in Amsterdam.
- Declared Data: Information directly and expressly supplied by a user to a party through meaningful interaction with that party.
- Examples would include most situations where a user is asked to enter data into a form for submission, such as a site registration process or contest entry form.

Vinay Goel

- Would your definition of declared data include either search queries or a user clicking on a 'Like' or '+1'? I like your examples of information provided on a site registration or contest entry form but think we need to be clearer to exclude search queries or clicks on Like/+1. I believe the user would consider both of those as observed behavior and not part of its registration with that party.

Shane Wiley

- The Search debate is a long and tortured one so I purposely attempted to avoid it. :)
- On the Like or +1 buttons, we've already decided as a group that once the user clicks on the button (meaningful interaction) that it falls under 1st party rules at that point. That said, I don't see a click on a Like button, an ad, or video player as declared data - the click is simply observed not a declaration of data from the user to the web site/service.

Rob Sherman

- How would your definition handle activities that a user intentionally shares but does not enter into a form? As an example, you can (explicitly) authorize Facebook to post a story to your timeline whenever you listen to a song on Spotify. This is information that a user has specifically instructed us to receive and use — and has instructed Spotify to provide -- but that is not "entered into a form" on each occasion.

Shane Wiley

- I believe that's fair and relies heavily on prior user consent for that observed activity to be converted to a declared one.

Agenda Nov. 14, 2012 Call

- 3. In the context of ISSUE-54, I'd like us to get a quick sense whether we can agree that Shane's definition of "declared data" from ACTION-306 is useful text This does not yet close ISSUE-54, but would at least permit us to have agreed vocabulary to talk about one of the elements of that issue.

John Simpson/ Alan Chapell Proposal March 31, 2013:

- Normative:
  - When DNT:1 is received:
    - A 1st Party MUST NOT combine or otherwise use identifiable data received from another party with data it has collected while a 1st Party.
    - A 1st Party MUST NOT share identifiable data with another party unless the data was provided voluntarily by the user and is necessary to complete a business transaction with the user.
    - A Party MUST NOT use data gathered while a 1st Party when operating as a 3rd Party.
- Non-Normative:
  - When DNT:1 is received, a 1st Party retains the ability to customize content, services, and advertising only within the context of the first party experience. A 1st party takes the user interaction outside of the 1st party experience if it receives identifiabledata from another party and uses that data for customization of content, services, or advertising.
  - When DNT:1 is received the 1st Party may continue to utilize user provided data in order to complete or fulfill a user initiated business transaction such as fulfilling an order for goods or a subscription.
  - When DNT:1 is received and a Party has become a 3rd Party it is interacting with the user outside of the 1st Party experience. Using data gathered while a 1st party is incompatible with interaction as a third party.

Post to list by John Simpson on April 8, 2013 about categories of data affected by append proposal.

(This post responded to questions posed by Peter Swire.)

Peter,

Thanks for setting out these data categories. In line below I outline what I believe should happen with data append when when DNT:1 is sent to a 1st Party site. It's my hope that the proposed data append text and current spec language accomplishes the goal, but it's possible that it misses the mark. This is what I intended the data append text to accomplish.

Thanks,
John

On Apr 3, 2013, at 12:47 PM, Peter Swire <peter@peterswire.net> wrote:
Based on discussions to date, here are some categoriesrelated to the "append" discussion. Perhaps I could ask the authors to consider which of these categories they believe would be covered by their proposals where DNT:1 is set at a 1st Party site? (Apologies if I have made any mistake on what is in the currentspec.)

Three major categories:
1. Data from a 1st Party
2. Data to a 1st Party

3. Data used by a 1st Party

Yes, I agree that when a 1st Party receives a DNT:1 message the compliance obligations would involve how the 1st party would handle each of the three categories of data listed above.

1. Data from a 1st Party

1.1. 1st Party to Outsourced Service Provider. Current spec allows this if there is no leakage. Data can only be "accessed and used as directed" by the 1st Party.

I agree the current spec allows data to flow to an outsourced service provider to be used only on behalf of and at the direction of the 1st Party. There needs to be ways to silo the data, etc. I believe our data append text allows this.

1.2. 1st Party to 3d Party. Current spec says "The first party must not pass information about this transaction to non-serviceprovider third parties who could not collect the data themselves under this standard."

I agree the the current spec prohibits 1st Party data to be shared with a 3rd Party who couldn't collect the data. This should remain the same under the data append text.

2. Data to a 1st Party

2.1. Data from public records. Example discussed of employee of the 1st Party using the telephone white pages to look up an address. A variation is where the 1st Party purchases information from a service about bankruptcy or other court records.

My view is that an employee of a 1st Party could use public data to augment data gathered from the network interaction while a 1st Party for out-of-band communication. So, in this case, the employee could determine based on the data gathered during the online interaction that it was necessary to telephone the user. He or she could look up the telephone number in the white pages and call them. What should not be allowed with DNT:1 enabled is for the offline data, be it from the white pages, bankruptcy or other court records to be combined with 1st Party data to shape the online network transaction.

2.2. Data from non-public records.

2.2.1. Dynamically use data to serve real-time ads.

This would not be allowed if DNT:1 is enabled.

2.2.2. Use data to supplement knowledge of 1st Party about a user, and use the updated set of information to serve online ads in the future.

This would not be allowed if DNT:1 is enabled.

2.2.3. Use data to supplement knowledge of 1st Party about a user, and use for purposes other than to serve online ads, such as update address and other contact information.

If this were for the purpose of out-of-band communication with the user, it would be allowed.

2.2.4. Use data to enhance 1st Party analytics, but don't target back to an individual user.

I'm sorry, I'm not sure what you envision here. Could you please give an example?

3. Data used by a 1st Party
3.1. Use in 1st Party context. Generally permitted under the spec.

Yes, a 1st Party is allowed to use data gathered in a 1st Party context for 1st Party interactions, including future ones.

3.2. Use in 3d Party context. Would be prohibited by Simpson/Chapell proposal.

Yes, I envision our text as prohibiting a Party to use data gathered as a 1st Party when it is a 3rd Party.

3.2.1. Personalized widgit – user sees a different widgit based on information known to the 1st Party.

This would not be allowed. It would have to be a generic widget. However, if the user had a meaningful interaction with the widget -- actually clicking on it and interacting as opposed to merely mousing over it -- the widget would become a 1st Party. If the widget were provided by a service that required a login, the widget, appearing as a 3rd Party could be personalized if the user remained logged in.

3.2.2. Personalized advertisement – user sees a different ad based on information known to the 1st Party.

Not allowed to personalize based on 1st Party info when in 3rd Party context.

3.2.3. Analytics or other scenarios?

I'm not sure I understand what analytics would be performed using data gathered as 1st Party when the site was in a 3rd Party context, but it would not be allowed under the data append proposal

One additional issue raised in the call: persistence of DNT header vs. header used for a particular network interaction.

I'm not sure I follow the point here. The DNT:1 header should be persistent. That is, once it's enabled it should remain enabled until the user turns it off, the user grants an exception or the site obtains out-of-band consent. It is conceivable that a user could visit a 1st Party site with DNT:1 enabled and return the next day with DNT:0. When DNT:1 is enabled, all of the data append compliance obligations would be in effect. If the user returned with DNT:0 they would not be.

Hope this is helpful.

Peter