Response to the Call for Objections on ISSUE-10
What definition of "Party" to use and where to include it

The questions before the group in this Call for Objections were what definition of "party," "first party," and "third party" to choose as the basis for the work of the Tracking Protection Working Group and in which specification document to include this definition.

Based on the comments submitted the co-chairs conclude that the Working Group has made the decision to define "party" as follows:

*"A **party** is a natural person, a legal entity, or a set of legal entities that share common owner(s), common controller(s), and a group identity that is easily discoverable by a user. Common branding or providing a list of affiliates that is available via a link from a resource where a party describes DNT practices are examples of ways to provide this discoverability.*
*Within the context of a given user action, a **first party** is a party with which the user intends to interact, via one or more network interactions, as a result of making that action. Merely hovering over, muting, pausing, or closing a given piece of content does not constitute a user's intent to interact with another party.*
In some cases, a resource on the Web will be jointly controlled by two or more distinct parties. Each of those parties is considered a first party if a user would reasonably expect to communicate with all of them when accessing that resource. For example, prominent co-branding on the resource might lead a user to expect that multiple parties are responsible for the content or functionality.
*For any data collected as a result of one or more network interactions resulting from a user's action, a **third party** is any party other than that user, a first party for that user action, or a **service provider** acting on behalf of either that user or that first party."*

This definition is consistent with the common understanding that the group has operated under for most of the past two and a half years. It is useful to recall that party definitions was one of the early controversies within the group: Some Working Group members argued that to qualify as a "party," a set of entities must operate under a common branding, such that an ordinary user would reasonably understand that they were the same company. On the other hand, some argued for a definition of party based more strictly on corporate affiliation: If two corporate structures were legally the same entity, then they should both be considered the same party under Do Not Track (provided that affiliation was easily discoverable. Eventually, many in the first group ceded this ground, and agreed to a broader concept of party.

This concept of first and third parties has been largely stable for most of the last two years. Recently, however, a significantly different definition of "party" was suggested by Working Group participant David Wainberg. Under his definition, two legal entities unaffiliated by corporate ownership or control could constitute one "party" if the entities enter into contract with other parties regarding the collection, retention, and use of data, and operated under some sort of common branding.

In the discussion and Call for Objections the Working Group, participants raised strong objections against this definition. Members noted that this definition suffered from a lack of clarity and was less likely to be consistent with user expectations. Questions about how such a definition would apply in practice were not fully explored, and the answers were not evident from the text of the proposal. Moreover, this definition marked a radical departure from the understanding that the Working Group had operated under for a long period of time.

A related question raised by the group was whether to include the definition of parties within the TPE. In order for the DNT signal to have meaning, it must be clear to whom the DNT flag applies. While the recently adopted definition of tracking does not include the term parties, the term "party," "first party," and "third party" appear throughout the TPE. This Call for Objection determines the

meaning of party for both documents, though ultimately the group may decide that the definition does not need to be included in the TPE spec if the semantics of the expression can be specified by other means. As the TPE currently includes at least the “same party” flag, it appears necessary to currently include this definition in order to get a comprehensive, adoptable, and self-contained TPE specification out to last call for implementation and testing. If the group decides to further reduce the dependance of the TPE specification on the compliance specification and lose the same party flag, the necessity to include a party definition has to be reassessed.

Definition Options

Two different definitions in normative text were put before the Working Group to make a decision. Additionally, the participants were asked for their objections regarding the location.

1. Option A: Common Ownership; First and Third Party

   A **party** is a natural person, a legal entity, or a set of legal entities that share common owner(s), common controller(s), and a group identity that is easily discoverable by a user. Common branding or providing a list of affiliates that is available via a link from a resource where a party describes DNT practices are examples of ways to provide this discoverability. Within the context of a given user action, a **first party** is a party with which the user intends to interact, via one or more network interactions, as a result of making that action. Merely hovering over, muting, pausing, or closing a given piece of content does not constitute a user's intent to interact with another party.

   In some cases, a resource on the Web will be jointly controlled by two or more distinct parties. Each of those parties is considered a first party if a user would reasonably expect to communicate with all of them when accessing that resource. For example, prominent co-branding on the resource might lead a user to expect that multiple parties are responsible for the content or functionality.

   For any data collected as a result of one or more network interactions resulting from a user's action, a **third party** is any party other than that user, a first party for that user action, or a **service provider** acting on behalf of either that user or that first party.

2. Option B: Common Ownership or Contract

   For unique corporate entities to qualify as a common party with respect to this document, those entities MUST be EITHER: commonly owned and commonly controlled OR enter into contract with other parties regarding the collection, retention, and use of data, share a common branding that is easily discoverable by a user, and describe their tracking practices clearly and conspicuously in a place that is easily discoverable by the user. Regardless, parties MUST provide transparency about what types of entities are considered part of the same party. Examples of ways to provide this transparency are through common branding or by providing a list of affiliates that is available via a link from a resource where a party describes DNT practices.

3. Document Location

   The participants were asked for objections to including the definition of tracking in either the TPE document or the Compliance document and to describe their objection.

The Call for Objections was open from November 8, 2013 to November 20, 2013. In total 11 members of the Working Group participated and presented arguments against or in favor of the options. The full results of the questionnaire are public at https://www.w3.org/2002/09/wbs/49311/tpwg-party-10/results

After careful weighing of arguments, the co-chairs have determined that the group has rejected Option B since it is vague, may be subject to abuse, and raises considerable privacy concerns.

Explanatory considerations on the choice of definition

The decision was made by exclusion. Based on assessing the substance of the objections against each option.

Objections against Option B:

Overall the Working Group did raise the more substantial arguments against Option B.

Mike O'Neill objects that Option B is "even vaguer than Option A. Entering into a contract or simply sharing a branding is far too loose a distinction to decide the context, and gives carte blanche for servers to arbitrarily decide it without regard for the user."

Jeffrey Chester voices similar concerns: "Entering into a contract is a please collect my data 24/7, cross all platforms card. There should not be a contract exemption for DNT."

This objection is also shared by John Simpson, who stated that a contract could make one party infinitely big: "As I understand this language ad networks could write contracts with sites, have the site display for example the DAA logo as a brand, include the DAA logo when it serves the ad, and everything would be considered the same site. Contracts and branding could make virtually 'every' site the 'same party.'"

Shane Wiley states in his objection comment that Option B would set "a horrible precedent for consumers by attempting to move 1st party relationships to contractual elements alone. The concepts of liability, accountability, and responsibility are lost in this approach and undermines already well understood and established definitions used today."

Additionally, he raises concerns that "this definition creates immediate misalignment with existing self-regulatory standards that many, if not all, industry participants in this Working Group already comply with through well established programs."

Rob van Eijk objects to link the concept of party with the concept of context since "context is user centric, no[t] corporate centric. For DNT to become a successful context negotiation mechanism it is essential not to pin down context without consulting the user first."

Objections regarding the wording of Option B are raised by David Singer and Amy Colando. David Singer considers the Option as "Insufficiently precise: "describe tracking practices clearly and conspicuously in a place that is easily discoverable by the user' doesn't seem well enough defined to be enforceable — what is 'clearly and conspicuously' and 'easily discoverable by the user'? Amy Colando states that the text of Option B would need further editorial modifications to be clarified.

In general, the co-chairs judge that these objections are significantly stronger than the objections raised against Option A. Either the language of Option B is vague and offers insufficiently clear guidance, or it would allow companies to align under one "party" banner to subvert the user's stated preference against cross-context tracking. This concept of a party runs counter to an ordinary user's expectations as well as the (previously) long-settled concept of parties within this Working Group.

Objections against Option A:

Option A also raised concerns regarding user privacy, although in total these were less substantial than the objections against Option B.

Jeff Chester considers common branding “insufficient“ since companies that operate multiple sites “require effective safeguards to ensure a consumer truly understands” online industry practices. Furthermore, “[h]aving two parties acknowledged as both First parties further weakens this spec. Few consumers would understand such joint arrangements and would likely have different motivations for visiting such a site. Jointly operated sites require a different approach, based on greater transparency and user control in order to qualify.” The chairs agree that the concern about multiple first parties is legitimate and subject to abuse; however, no plausible alternative formulation was proposed. Option B was silent on the issue of multiple first parties and arguably allowed for them as well.

Brooks Dobbs argues that Option A would not “adequately preclude[…] a single ‘party’ from having various constituent parts under different control and with different policies.” The chairs do not deem this to be a strong objection, as under Option B, a single corporate entity with disparate affiliates and privacy practices would also qualify as one party.

John Simpson objects the wording of ’easily discoverable by the user’ and suggests “a group identity that is ’obvious’ or ’apparent’ to a user. A user should not have to seek this information out; it should be immediately clear.” This objection applies no more to Option A than it does to Option B as well.

Mike O’Neill writes: “If there are different requirements on a receiving server depending on which role it assumes then the criteria to decide is far too vague. A user may not have intended to interact with any party, and even if they did a server could not know that. If there are less stringent requirements for first parties then the tendency will be to claim to be one.” As with the previous objections, this applies at least as strongly to Option B as it does to Option A. This seems to be more of a criticism of defining first and third parties (or contexts) at all, which was not proposed to the group as an option.

Some Working Group members are concerned that Option A would be nonconforming with existing legal regimes. Rob van Eijk writes: “Although at first sight, option A may look like (an attempt of) an analogy of the EU approach of data controller/processor, it is not.” John Simpson writes: “I am still trying to understand how a website would be controlled by distinct parties where all could claim to be first parties. It seems to me you have only one data controller and that would be the only first party.” The co-chairs point out that the specification will need to be globally applicable. Therefore, complete alignment with one regional legislation is not favorable. Also, as above, these criticisms also apply to Option B, which allows for corporate affiliation (along with discoverability) alone to make two commonly-owned entities one party.

David Wainberg offers a critique of the fairness of the Option A definition. “It needlessly, without a relevant privacy-related rationale, discriminates against small independent companies that are affiliated by means other than ownership, and that may have substantial privacy protections in place. Compare these two examples:
1. A network of typosquatting or search spam sites that commonly owned, along with a third party ad network, but without common privacy policies. In fact, they are without any user-visible privacy policy, and without any common branding except a list of affiliates linked from the footer. Under Option A, because the sites are commonly owned they can collect and use data across their entire network of sites, without regard to DNT.
2. A network of independent political blog publishers are affiliated by contract to use a third party to share data, and enable high value targeted ads across the network. The sites provide prominent

notice of this to users that indicates data is being shared, and that makes a common set of strict privacy promises to users. Under this definition, the sites would be limited by DNT.
Obviously, the 2nd case would be a better experience for users. We should therefore create an opportunity and incentive for independent sites to adopt such models. Option A does not create such incentives."

The chairs acknowledge that in Scenario 1, under either party definition, a user may be tracked in ways that are contrary to her or his expectations. No definition was ultimately proffered to address that scenario. However, just because Do Not Track does not solve all online privacy issues, does not mean that it should be defined to exclude other scenarios where a user would expect Do Not Track to apply. Ultimately, Option B was defined very broadly, and could be interpreted to fundamentally subvert the purpose of the Do Not Track signal. Working Group members for a long time have recognized a logical distinction between companies with who the user has a direct relationship (at least in the context of that relationship) and those with which she doesn't. Option B could allow a broad range of companies with no relationship to the user to claim first party or same party status merely through an undefined branding relationship and common (but wholly undefined) privacy practices.

Alan Chapell and Jack Hobaugh also object the concept of ownership as a meaningful basis to constitute parties. Alan Chapell writes: "An over reliance upon the fiction that ownership equates to sound privacy practices creates incentives for consolidation. Big companies will get even bigger – resulting in more data collection across a small number of Internet behemoths. Given the significant risk that large first parties will be exempt from DNT, it is difficult for any reasonable observer to understand how this will serve consumer privacy interests. In short: a good deal of current business practices will continue regardless of DNT status. The only change will be the types of entities doing the tracking. Multiple factors should be considered (e.g., context and sensitivity of the types of data collected) when evaluating the efficacy of a privacy approach, instead of relying on the outdated first/third party distinction." Jack Hobaugh argues similarly: "I also object to the extent that these definitions suggest that privacy gains can only be obtained through common ownership. I incorporate by reference, the section "harm to competition" found at http://www.w3.org/2002/09/wbs/49311/datahygiene/results."

This objection identifies a legitimate privacy issue: Under Option A, there may be relatively stronger incentives and opportunities for large first parties to accumulate more comprehensive databases about individuals than today, as opposed to the status quo or Option B where the incentives would skew (again, relatively speaking) more toward third parties and the accumulation of various distributed (and likely less comprehensive) behavioral databases. While the chairs appreciate this concern, we judge that the considerable privacy advantage of applying a more narrow and intuitive definition of parties outweighs the privacy risk of marginally greater incentives toward larger first party databases.

Option A also received editorial comments that pointed out that the option may need further non-normative clarification.

Jeff Chester wrote that the definition of "intends" "must be conditioned by an analysis of the content used to bring the user to the site. Practices where users are sent to a site due to rich media driven and immersive ads or e-discount coupons require a different approach."

Amy Colando criticized that "the distinction between first and third party should rely on reasonable, objectively determined criteria, rather than subjective determination of a user's intention."

David Singer pointed out that the "bracketing of the first sentence could be clearer: is either (a) a natural person or (b) a legal entity or (c) a set of legal entities that share common owner(s), common controller(s), and a group identity that is easily discoverable by a user."

The group may subsequently consider the need for non-normative language to clarify this definition, but these editorial comments did not pose stronger objections than the objections to Option B.

Based on these comments received in the Call for Objections, the co-chairs conclude that Option B raised more substantial concerns than Option A.

Explanatory considerations on the choice of location

The second question before the Working Group was where to include the definition of parties.

The answers raised some objections against including the definition within the TPE specification.

Rob van Eijk, and similarly Mike O'Neill and John Simpson, wrote: "TPE doesn't need a party defintion in order to stand on itself. […] In order to move the TPE to last call, it is best in my view not to overload the TPE with the many interlinked and unresolved compliance document discussions related to party. "

Brooks Dobbs stated: "Technical definitions make sense in the TPE, and compliance definitions make sense in a compliance document(s). If we find that the TPE is reliant on non-technical definitions then we have essentially found that the documents can't be meaningfully separated, which would seem in conflict with the choices offered by the last poll."

Jack Hobaugh objects the inclusion because the "TPE should remain a pure protocol and technical specification document. Some have contended that some TCS definitions are needed in the TPE in order for the user to understand the choice that the user is making regarding the DNT signal. This is simply not the case. A technical specification need only specify the requests and responses necessary for a DNT protocol to be implemented in a scalable and implementable solution across all browsers and the servers called. A technical specification should not inform the user regarding a policy or compliance choice but instead should inform the technical community on how to implement a technical solution. The compliance specification for the DNT signal should be left to the compliance regime, whether it is a national compliance regime, a W3C-based compliance regime or an industry-based compliance regime. Porting definitions from a particular compliance regime into the TPE only serves to provide an incomplete and confusing picture to those attempting to implement the technical protocol."

John Simpson argues that "it would raise the question of why some would be listed and not others".

The chairs note that only a few Working Group participants objected to the inclusion of a party definition in the TPE. On the other hand, depending on how the TPE is ultimately structured, the meaning of the DNT signal may be contingent upon a concept of party. Without such a definition, it could be unclear from the semantics of the DNT signal to whom the signal applies. Currently, the definition of tracking does not rely upon a definition of party, but elsewhere the TPE extensively uses the terms "party," "first party," and "third party" and includes a flag indicating "same party." In order to get a comprehensive, adoptable, and self-contained TPE specification out to last call for implementation and testing we conclude that the most important semantics need to be provided to make the TPE a workable specification. The concept of party is now defined for both TCS and TPE, although ultimately the group may decide that TPE does not need to use the term "party" (or "first" and "third" parties) at all. Consistent with the distinction between TPE and TCS, the TPE should not specify substantive compliance obligations for either first or third parties.

Result

In conclusion, *ISSUE-10, What is a first party?*, is hereby closed, and the following definition will set the outline for the group's continued work and will be included in TPE:

"A **party** is a natural person, a legal entity, or a set of legal entities that share common owner(s), common controller(s), and a group identity that is easily discoverable by a user. Common branding or providing a list of affiliates that is available via a link from a resource where a party describes DNT practices are examples of ways to provide this discoverability.
Within the context of a given user action, a **first party** is a party with which the user intends to interact, via one or more network interactions, as a result of making that action. Merely hovering over, muting, pausing, or closing a given piece of content does not constitute a user's intent to interact with another party.
In some cases, a resource on the Web will be jointly controlled by two or more distinct parties. Each of those parties is considered a first party if a user would reasonably expect to communicate with all of them when accessing that resource. For example, prominent co-branding on the resource might lead a user to expect that multiple parties are responsible for the content or functionality.
For any data collected as a result of one or more network interactions resulting from a user's action, a **third party** is any party other than that user, a first party for that user action, or a **service provider** acting on behalf of either that user or that first party."