Call for Objections on Issue 22 (Other Party Property)

V01, 2017-06-14

Alternative Resolutions for Issue-22 under Consideration

Option (A): Add field otherParty to Tracking Status resource:

Add *the text below to the TPE after the same-party section.*

It might be useful for a site to distinguish between domains that are not subject to their own control.

An origin server MAY send a property named "other-party" containing an array of objects each with a string property “domain” whose value represents a particular domain name that the origin server claims to include (i.e. not referenced by the "same-party" property and do not share the same data controller indicated by the “controller” property).

Each object MAY also include other properties , e.g. a string property “controller-name” indicating the name of the entity responsible for the domain, or an array property “purpose” indicating the list of one or more purposes for which data is claimed to be processed.

Option (B): Close issue 22 without changes to the TPE

Inputs Received

Objections to Option (A): Add other party property

Responder	Objections to Option A: Add Other Party Property
Apple, Inc. (David Singer <singer@apple.com>)	I have several objections to this proposal. 1) There is no connection of this field to the subject of the specification, which is the Do Not Track signal and its support. No mandatory or even optional processing by any agent (particularly the user-agent) is stated (e.g. "The UA MAY do x"). As such it is out of scope. 2) The list seems to include some of the other parties that might or might not appear in an interaction with this site. As such, it can be 'wrong' both by inclusion (mentioning sites a vist does not encounter) and omission (not mentioning sites that are encountered). This means it can be effectively, completely wrong. It's not clear what requirements, if any, apart from syntactic correctness, are placed on this list. What MUST it include? What

Responder	Objections to Option A: Add Other Party Property
	MUST it omit? The "i.e." implies that parties in the same party array MUST NOT occur here, but this is not stated normatively. 3) It's not clear what the site is 'claiming' when it 'claims to include' another site, and therefore what, by implication, it is not claiming for sites that are not in the list. 4) The list purports to be able to express the controller of the third parties, which is wrong. We should not have one party speak to the formal status of a party not under its control. If the UA wants to discover the controller of a site reliably, it should interrogate that site, not rely on a statement from an unaffiliated site.
Roy Fielding (Adobe)	Adobe objects to Option A because the proposed text is a placeholder for something to be defined later that is currently disconnected from TPE. It serves no purpose in the existing protocol; presumably, based on what has been implied by the discussion, the intended purpose is to provide information specific to an imagined user interface for a mechanism of configuration of some form of selective blocking. However, the terms being used here are inadequately and inconsistently defined for that purpose, at least partly because the WG decided not to use region-specific legal terms (such as those in the GDPR) for TPE to avoid making the protocol region-specific. We don't need to predefine such a property. The TSR representation is already defined to be extensible, specifically through the addition of new properties that might or might not be required by some set of compliance regimes. It is entirely possible for this under-specified feature to be completely specified in a compliance specification without any change to TPE, authored by anyone, and capable of using defined legal terms consistent with a given region. As such, Option B is preferred.
Shane Wiley (Yahoo)	I continue to recommend we not add "otherParty" at this time as currently scoped, defined, and intended for use. **Issue 1: otherParty doesn't impact the DNT signal in any way.** As we've discussed on the mailing list to meet the requirements for Consent under GDPR options already provided under the TPE cover those needs.

Responder	Objections to Option A: Add Other Party Property
	- SameParty Array: any domains, both 1st and 3rd party, can be accommodated with this feature which is already available. For example, a 1st party requesting a site-wide exception can list it's 3rd party domains in this list so they receive DNT:0. ANY party not in this array will receive the user's default DNT value. Assuming that's DNT:1 then domains not listed in the SameParty array during a User Granted Exception will receive DNT:0. The otherParty doesn't change or assist in the DNT signal a party receives - in any way. It is proposed as a list of domains that are not under contract with the 1st party but because the 1st party is aware of them it would like to list them for transparency purposes - but not changing the default DNT signal they receive. It's this very specific disconnect with DNT that suggests this is not an appropriate addition to the DNT standard. - TSRO: The tracking status response object already provides the opportunity to link to a list of 3rd parties in human readable form. The desire to provide a machine readable list is addressed in Issue 2. **Issue 2: otherParty is a Tracking Protection White List.** As discussed in the email list the desire for a machine readable list is specifically to allow the web browser to take some action with respect to that list - blocking was mentioned as one outcome of any domain that is not found in the sameParty or otherParty arrays. The WG spent considerable time discussing the pros/cons of Tracking Protection Lists and becoming involved in domain blocking. This resulted in the group unanimously agreeing to drop the pursuit of this path. Again, to be as clear and plain as possible, otherParty is intended to be a blocking list - not a transparency tool - in my opinion based on the need for machine readability and the email discussion on the intention of browser intervention based on domains listed. I don't want to discourage this pursuit more broadly and support the desire to add privacy tools that provide greater transparency to users over what already exists today between browser tools, controls, and add-ons available in the market. Attempting to use DNT to add none DNT relevant elements in not the correct path to arrive there IMHO. I would recommend a new working group be formed to discuss broader transparency tools that can live outside

Responder	Objections to Option A: Add Other Party Property
	of the use of DNT and in that context a group can more thoroughly look at all possible elements of transparency that could become available in both human and machine readable form (P3P v2?).

Objections to Option (B): Close without Change

Responder	Objections to Option B: Close Issue 22 with no change
Aleecia McDonald	Strong preference for option A We have a DNT standard that violates user expectations by continuing to collect data for users who have opted out of tracking. We compound this by not providing sufficient transparency for functionality by any party. This proposal strengthens user consent and transparency, particularly with regard to multiple parties (a rather common use case.) N.B. David Singer's concerns are non-trivial. Were there a preference for "yes, but editors make this better drafted please" I would take that path. As it is, flawed A is better than the toxic silence of B. With A, it can be used for good with likelihood of some exasperating actors. With B, users just lose all the time.
Center for Democracy and Technology (Joseph Hall <joe@cdt.org>)	This seems like a useful option to have available for publishers, although we agree with our Apple colleagues that it's unclear what an array of "other parties" will actually mean. However, there doesn't appear to be much harm associated with including this and if the EU or other entities develop ad-hoc or other standards on how publishers targeting their citizens might use this effectively, we have no objection and would like to see room for innovation in more automated forms of consent and tracker information communication.

Responder	Objections to Option B: Close Issue 22 with no change
Chris Pedigo	Hi Matthias – I cannot participate in the poll as our W3C membership has lapsed. But, as a trade association representing 80+ premium publishers, we object to Option B because we support having a machine-readable TSR. It will be useful for publishers that must comply with the GDPR, and potentially the ePrivacy Directive. Publishers are not likely to ask for web-wide consent. Instead, they would likely ask consumers for site-wide consent for themselves and a select number of 3rd party partners. Having a machine-readable TSR would allow the browser to block unauthorized 3rd parties in real time from tracking consumers.
Electronic Frontier Foundation (Alan Toner <at@eff.org>)	Option B neglects the need for greater transparency regarding the parties present on a website and the delivery of comprehensive information in a form suitable for examination and action by a user agent. The user needs information in a machine-readable form so as to enable practical decision-making about their privacy choices. The 'other parties' field offers publishers a compliance framework for the consent requirements under EU law whilst reducing the opportunities for malware and the leakage of user data.
Institut National de Recherche en Informatique et en Automatique (Nataliia Bielova <nataliia.bielova@inria.fr>)	Objection to Option B By not having an "other-party" property, the publisher doesn't have an easy way to communicate the list of embedded third parties to the user agent, therefore reducing its possibility to provide privacy-friendly implementation of the publisher's server. I agree with EFF and CDD that "the 'other parties' field offers publishers a compliance framework for the consent requirements under EU law whilst reducing the opportunities for malware and the leakage of user data." Moreover, even though GDPR and ePR are EU laws (that are nevertheless applied to all the countries

Commented [JD1]: IMHO This can be done today with user-granted exceptions that may list a set of URLs that are to receive DNT;0 on that site. However, unlike TSR info, this is not retrievable before visiting the site.

Responder	Objections to Option B: Close Issue 22 with no change
	that provide services to persons who are physically located in the EU), I would like to remind that the main motivations for the chapter's extension was "help web-sites to achieve privacy compliance in the EU ".
Jeffrey Chester (CDD)	CDD believes that online users must have information in a machine-readable manner in order to support meaningful and practical decision-making regarding their choices for privacy. Option B does not provide the range of transparency necessary to inform about the parties who can be present at a website. Users need to have comprehensive information in a format that can be examined and acted upon by a user agent. We agree with our EFF colleague that "the 'other parties' field offers publishers a compliance framework for the consent requirements under EU law whilst reducing the opportunities for malware and the leakage of user data."
John Simpson (Consumer Watchdog)	Objection to Option B Consumer Watchdog maintains that online users must have information in a machine-readable manner in order to support meaningful and practical decision-making regarding their choices for privacy. Option B does not provide the transparency necessary to inform about the parties who can be present at a website. Users need to have comprehensive information in a format that can be examined and acted upon by a user agent. We agree with CDD and our EFF colleague that "the 'other parties' field offers publishers a compliance framework for the consent requirements under EU law whilst reducing the opportunities for malware and the leakage of user data." It is imperative that Do Not Track options provide consumers meaningful choice and control. A DNT

Responder	Objections to Option B: Close Issue 22 with no change
	standard that falls short of the promises implied by its name ultimately undermines users' trust in the Internet.
Mike O'Neill (Mike O'Neill <michael.oneill@baycloud.com>)	I object to Option B because not having an "other-party" property restricts the ability of servers to convey relevant data to help user agents protect the security and privacy of users. Like the "same-party" array property, "other-party" is an optional piece of machine-readable data that servers can convey to user agents, extensions to user agents, regulatory scanners or other software systems acting for or in the interests of users. It is meant to convey a list of domains of subresources that the site is designed to host, or that the site controller is aware may appear. If the array is there and a domain appears that is not on this list, not on the same-party list, and has not been explicitly been given consent to by the user, then appropriate action can be taken, such as exclusion. The obvious potential use is malware detection, but there is also a use case for online advertising. Because the property is contained in a data structure designed to be created dynamically according to request header input it naturally allows a different set of domains to be indicated if the user has given their consent or not, which ad exchanges or intermediaries can utilise to ensure legal compliance. No other mechanism can enforce anti-malware security without severely restricting functionality based on third-party elements. The Content-Security-Policy API only applies to the current browsing context, and Embedded Enforcement would not be easy for many sites to take advantage of, and is anyway not currently available. Neither of these APIs can differentiate interactions based on user consent. This is nothing like the Tracking Protection lists that Microsoft introduced years ago, the similar

Responder	Objections to Option B: Close Issue 22 with no change
	system that Mozilla introduced last year for Firefox, the analogous content blocking capability that Safari provided 2 years ago or the host of content blocking extensions. These are mainly based on “blacklists”, which can be difficult to keep up to date and can be "gamed" for commercial purposes, and are all web-wide, without the ability of sites to benefit from gaining the trust, and therefore the explicit consent, of their users. The “other-party” array is a “whitelist”, site-specific and optional. The “same-party” array is similar, but for domains that are either managed by the data controller(s) or their data processors. The "same-party" property also leaves user agents etc. the option to act on it (and the TPE explicitly mentions the possibility of exclusion). The “other-party” array lets sites simply expand this list of domains to those that it does not control, but expects may be present. This improves the ability of user agents to inform users of what is happening on a page, and allows sites to enable user agents to safeguard users interests in a systematic way.
Rob van Eijk (Rob van Eijk <rob@blaeu.com>)	I object to Option B. I remark the following. A main focus of our work throughout the extended implementation phase is "to demonstrate the viability of TPE to address the requirements for managing cookie and tracking consent that satisfies the requirements of EU privacy legislation". This focus should lead - IMHO - to a major improvement of the TPE, compared to the current draft. The 'other-parties' property leads to better privacy protection and a user-friendlier browsing experience with less consent dialog boxes. Providing information is a cornerstone in the EU legal framework, not just for informed consent, but also when personal data is processed under other legal grounds, e.g. the legitimate interest

Responder	Objections to Option B: Close Issue 22 with no change
	legal ground. Information is required under the GDPR, the ePrivacy Directive, and the proposed ePrivacy Regulation. The 'other-party' properties provides a meaningful way to be specific about embedded resources: (a) the modalities of the collection, (b) its purpose, (c) the person responsible for it and the (d) other information required under the GDPR where personal data are collected, as well as (e) any measure the end-user of the terminal equipment can take to stop or minimize the collection. In sum, the 'other-parties' property is a crucial building block in the EU legal framework. It complements other properties in the Tracking Status Representation, e.g., the 'same-party', and 'controller' properties.
Vincent Toubiana (Vincent Toubiana <vtoubiana@cnil.fr>)	Other parties are already identified In most cases, this fields will simply list the domains that are already present in the Content Security Policy, hence the burden for the publisher will be minimal. Unlike the CSP which is “technically binding”, the “other parties” filed may be legally binding. Improving Consent Other party should not be seen as a blocking list, it would be quite the opposite as it will help obtaining a valid consent. The « other-party » field will help website to obtain a valid consent as they will be able to specify purposes for tracking. Furthermore, if the user can specify that he's okay to be tracked for specific purpose, parties listed under "Other party" for that purpose will not have to obtain consent again.
Walter van Holst	- It would reduce transparency - An other-party-array allows for a more nuanced approach to compliance with EU-legislation, without it it is quite well possible that the TPE has lost its

Responder	Objections to Option B: Close Issue 22 with no change
	usefulness for EU-compliance purposes entirely. I would like to emphasize that the DNT;1 and DNT;undefined signals are meaningless in a EU context, where only DNT;0 matters. Having the ability to extend the TPE and yet-to-be-defined compliance specification is a cop-out from this WG's responsibility. The TPE is there to define the signals, any future TCS may define the legal implications of the signals, but should not perform any roles the TPE already can fulfil since that would create a chicken-and-egg problem.

Discussion

Objections Summarized

Objections against Option A: Add otherParty

- Unclear semantics of the field: What does it mean if an otherParty is included? (David Singer, Roy Fielding, Joe Hall)
- No link to the behavior of the site or the user agent (David Singer, Roy Fielding)
- The information can be communicated today. The field only adds machine readability. (Shane Wiley)
- By means of the machine readability, it might be mis-used as a whitelist for blocking. (Shane Wiley, Chris Pedigo, Mike O'Neill)
- Replicates the information that can be published as the CSP (Vincent Toubiana)

Objections against Option A:

- otherParty is essential to provide additional transparency in a standardized way (John Simpson)
- otherParty fosters innovation towards more automated handling of consent and tracker information (Joseph Hall).
- otherParty allows publishers to retain control over their sites by inform users what elements they expect to be present (Chris Pedigo)
- otherParty offers a compliance framework for consent in the EU (Nataliia Bielova, Jeff Chester, Alan Toner,Rob van Eijk)
- otherParty provides machine-readable and actionable information for user's decision making (Jeff Chester, John Simpson)
- Without sufficient choice and control, user's trust is undermined (John Simpson)
- otherParty is meant to convey a list of domains of subresources that the site is designed to host, or that the site controller is aware may appear. (Mike O'Neill)
- [Unlike the information in user-granted exceptions], the otherParty field can be generated dynamically to convey better information (Mike O'Neill)
- otherParty reduces the risk of malware and user data leakage by telling a user agent what URLs a publisher trusts (Alan Toner)

- otherParty can enable user-agents to implement fine-grained and publisher-controlled blocking that is better than today's blacklists (Mike O'Neill, Chris Pedigo)
- Leads to better privacy protection (Rob van Eijk)
- Providing information is a cornerstone of the EU legal framework (Rob van Eijk)
- The 'other-party' properties provides a meaningful way to be specific about embedded resources: (a) the modalities of the collection, (b) its purpose, (c) the person responsible for it and the (d) other information required under the GDPR (Rob van Eijk)
- otherParty allows to specify purposes for tracking (Vincent Toubiana)
- Having the ability to extend the TPE and yet-to-be-defined compliance specification is a cop-out from this WG's responsibility. (Walter van Holst)

Condensed Summary of Arguments

The goal of a call for objection is to identify the option with the least substantiated objections. The goal is to find an option that the working group can live with. This forces us to ask the question "what choice has the least negative consequences".

Pro: EU Compliance – Meeting our chartered objective

The objections against option B (no change) were plentiful. The main message was that additional machine-readable information is essential to meet our chartered objective to help with EU compliance. Another input (Walter van Holst) was that additional fields such as purpose may be needed.

Pro: Actionable by User Agent

Another important area of comments was that without machine-readable information, user agents are not enabled to act and provide protection against malware and automated management of privacy. One point was that machine-readability simplifies archiving of informational fields to document the context of a user-granted exception.

Mixed: Potential Use for Blocking

The respondents indicated that otherParty can be used for whitelisting. This was seen as a risk (enabling a behavior that is out of scope and hurts sites) and also as a benefit (preventing untrusted content from loading; allowing publishers to better constrain undesired content from being loaded on their site).

Contra: Technically Immature

Some respondents indicated that the proposal is not technically mature. Comments were lack of semantics, the current data structure just being a beachhead for further data additions, and the fact that it is unclear whether the field should affect browser behavior.

Contra: Redundant with Existing Mechanisms and Extensibility

People observed that the machine readable field otherParty only adds machine-readability to other fields that may convey the same information. Furthermore, the new field adds a-priori-discoverability to the existing mechanism where sites can list URLs when they ask for an exception. Finally, Roy observed that the TSR is extensible and any field can be inserted by sites to create a de-facto standard. Others were not aware of this extensibility.

Discussion and Proposed Consensus

The goal of a call for objection is to identify the option with the least substantiated objections. The goal is to find an option that the working group can live with. This forces us to ask the question “what choice has the least negative consequences”.

In order to reach our chartered objective, the conclusion is that we need to add additional information-only field to satisfy the transparency requirements of the emerging regulation. However, there is a high risk that the current text proposal is not clear enough and not sufficient to satisfy the emerging requirements (i.e. more fields may be needed).

To ensure that we meet our chartered objective, we believe that the option “no change” has stronger substantiated objections and it is important to allow additional information fields to meet our chartered goal. However, we also understand that the risks of standardizing a premature solution are high if we move before gathering more implementation experience.

We suggest the following consensus:

- Continue developing the right set of informational fields to add to the TSR (via the existing ability to extend the TSR) that meet the transparency requirements of the emerging EU regulation. Such best practices should be published as a note and once a consensus evolves may be integrated into future versions of this standard.
- To push this approach and the extensibility emphasized by Roy, we suggest to change the TPE by introducing the following note:

> The tracking status object can be extended by adding additional informational properties or by defining additional tracking status values. We require that extensions introduced SHOULD be defined and documented by a policy document referenced by the URL in the policy property field.
>
> Note: One goal of this extensibility is to enable variations by policy and the evolution of best practices for the emerging EU regulations.