Working Draft: This document seeks to provide links to previous discussions and proposed text with regard to service providers within the Tracking Protection Group. We apologize for any missed text or viewpoints or for including any issues unrelated to service providers.

Service Provider

3.4 Service Providers (Barebones)

http://www.w3.org/2011/tracking-protection/drafts/CambridgeBareBones.html

Note: We do not expect outsourcing to be a major topic of discussion at the Cambridge face-to-face, so this definition is suggested as a placeholder. Some working group participants have argued for more prescriptive rules to qualify as a service provider.

Outsourced service providers are considered to be the same party as their clients if the outsourced service providers only act as data processors on behalf of that party in relation to that party, silo the data so that it cannot be accessed by other parties, and have no control over the use or sharing of that data except as directed by that party.

Service Provider/ Outsource Definition (Full Text)

http://www.w3.org/TR/tracking-compliance/#def-service-providers

3.4.1 Option 1: Service Provider/Outsourcer Definition

A first party or a third party *MAY* outsource functionality to another party, in which case the third party may act as the original first party or third party under this standard, with the following additional restrictions:

- Data collected by each outsourced company is separated for each party they collect data for by both technical means and organizational process, AND
- The outsourced company has no independent rights to the collected information, AND
- A contractual relationship exists between the outsourced and the party they collect data for that outlines and mandates these requirements.

An outsourced company acting on the behalf of another party is subject to all of the same restrictions on that party (for First or Third party, as appropriate.)

3.4.2 Option 2: Service Provider/Outsourcer Definition

Outsourced service providers are considered to be the same party as their clients if the outsourced service providers only act as data processors on behalf of that party, silo the data so that it cannot be accessed by other parties, and have no control over the use or sharing of that data except as directed by that party.

3.4.3 Option 3: Service Provider/Outsourcer Definition

Service Providers acting on the behalf of a First Party and with no independent rights to use the First Party's data outside of the context of that First Party and Permitted Uses are also considered to be acting as the First Party.

http://lists.w3.org/Archives/Public/public-tracking/2012Jul/0141.html

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?

http://www.w3.org/2011/tracking-protection/track/issues/49

Shane's Definition:
http://lists.w3.org/Archives/Public/public-tracking/2012Sep/0154.html

A Third-Party MAY operate under the rules for a first party if the following conditions are met:

- Data collected is separated for each First Party by technical means and organizational process, AND
- The Third Party has no independent rights to the collected information outside of Permitted Uses (see Section X.Y), AND
- A contractual relationship exists between the Third Party and the First Party that outlines and mandates these requirements.

A Third-Party acting on the behalf of a First Party is subject to all of the same restrictions of a First Party.

A Third-Party MAY operate as a Service Provider to another Third-Party if the following conditions are met:
- Data collected is separated for each supported Third Party by technical means and organizational process, AND
- The Third Party has no independent rights to the collected information outside of Permitted Uses (see Section X.Y), AND
- A contractual relationship exists between the Third Party and supported Third Party that outlines and mandates these requirements.

A Third-Party acting on the behalf of another Third-Party is subject to all of the same restrictions of a Third-Party.

[NOTE - I purposely approached the above language in a "template fashion" as I believe it's possible to consolidate this down to "any party operating on the behalf of another party" and keep the same language.]

<Non-Normative>

Third Parties that act purely as vendors for their customers (First Parties in this context) are not the intended target for the Tracking Preference Expression but it's important there are no unintended activities that are extended to a Third Party through this allowance. In all cases, its expected a Third Party acting on the part of a First Party follows all of the same restrictions placed on a First Party.

For the data separation requirement, Third Parties have technical options to achieve appropriate separation but in each the critical element is that data is never reconstituted for users that have shared a Tracking Preference. On possible approach would be to leverage a per partner hash against a common cookie identifier, ensuring the resulting identifier is consistent for a specific First Party but is unable to be linked with another First Party's identifier.

Contractual requirements that enforce data rights and responsibilities for separation are a critical element of establishing a Third Party as acting on a First Party's behalf. Contracts may occur directly through parties (for example, a Publisher in an Ad Network) or between intermediaries (for example, an Ad Network acting through an Ad Exchange). In either case, data separation and removal of independent rights are necessary elements that must survive intermediary contractual constructs.

Jonathon Mayer’s Non-normative examples:

http://lists.w3.org/Archives/Public/public-tracking/2012Mar/0298.html

I. Technical Precautions

A. Siloing in the Browser

Outsourcing services should use browser access control features so that stored data specific to one first party is never accessed or collected when the user visits another first party.

i. Same-Origin Policy

The same-origin policy silos stored data by domain name. An outsourcing service can use a different domain name for each first party.

Example: Example Analytics provides an outsourced analytics service to Example News and Example Sports, two unrelated websites. Example Analytics stores its cookies for Example News at examplenews.exampleanalytics.com, and it stores its cookies for Example Sports at examplesports.exampleanalytics.com.

An outsourcing service could also use the first party's domain.

Example: Example Analytics stores its cookies for Example News at examplenews.com, and it stores its cookies for Example Sports at examplesports.com.

ii. Cookie Path Attribute

The HTTP cookie path can be used to silo data to a first party.

Example: Example Analytics stores its cookies for Example News with "Path=/examplenews", and it stores its cookies for Example Sports with "Path=/examplesports".

iii. Storage Key

For key/value storage APIs, such as Web Storage and Indexed Database, an outsourcing service can use a different key or key prefix for each first party.

Example: Example Analytics stores data for Example News at window.localStorage["examplenews"] and data for Example Sports at window.localStorage["examplesports"].

B. Siloing in the Backend

i. Encryption Keys

An outsourcing service should encrypt each first party's data with a different set of keys.

ii. Access Controls

An outsourcing service should deploy access controls so that only authorized personnel are able to access siloed data, and only for authorized purposes.

iii. Access Monitoring

An outsourcing service should deploy access monitoring mechanisms to detect improper use of siloed data.

C. Retention in the Backend

An outsourcing service should retain information only so long as necessary to provide necessary functionality to a first party. If a service creates periodic reports, for example, it should delete the data used for a report once it is generated. An outsourcing service should be particularly sensitive to retaining protocol logs, since they may allow correlating user activity across multiple first parties.

II. Business Precautions

i. Policy

An outsourcing service should establish a clear internal policy that gives guidance on how to collect, retain, and use outsourced data in compliance with this standard.

ii. Training

Personnel that interact with outsourced data should be familiarized with internal policy on compliance with this standard.

iii. Supervision and Reporting

An outsourcing service should establish a supervision and reporting structure for detecting improper access.

iv. Auditing

External auditors should periodically examine an outsourcing service to assess whether it is in compliance with this standard and has adopted best practices. Auditor reports should be made available to the public.

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

http://www.w3.org/2011/tracking-protection/track/issues/73

Language from Jonathan Mayer and David Wainberg (Nov. 2011)

http://www.w3.org/2011/tracking-protection/track/actions/28

(ACTION-28, ISSUE-23)

Mayer - The text below reflects (I think) our consensus in Santa Clara on outsourcing.

If a first-party website outsources functionality to a third-party website, the third party may act as a first party under this standard so long as all of the following conditions are met when responding to a Do Not Track request.

1) The third-party website takes reasonable technical precautions.

Non-normative: One component of reasonable technical precautions may be using the same-origin policy to segregate information for each first-party customer.

2) The third-party website makes public commitments in a form that renders them legally enforceable by its first-party customer, individual users, and regulators.

This leaves at least four open sub-issues on outsourcing:

1) What is the scope of "outsourcing"? Is the third party just stepping into the first party's shoes? Or does it have some independent discretion in using data for its own purposes (e.g. for "product improvement" and "aggregate statistics" as Shane and Jules have proposed)? Here's my language from earlier in the month:
> -the third party will not use the data it collects except as directed by the first party

> -the third party will only use the data it collects to provide functionality to the first party; it will not use the data it collects for its own purposes
> -the third party will not share the data it collects except with the first party
> -if the first party requests, the third party will promptly delete the data it has collected
> -if the first party closes its account, the third party will promptly delete the data it has collected

2) What are the third party's technical precautions for? Preventing the collection of cross-site tracking data? Siloing data per first-party customer?

3) What are the factors that go into a reasonable technical precaution? (Note: this depends on what the precaution is for.) Here's my old language:
> -the extent to which the technical precautions prevent the collection of cross-site tracking data
> -whether the technical precautions are externally verifiable
> -the extent to which the technical precautions impede the third-party website's other functionality

4) Is there a MUST or SHOULD for reasonable internal controls? Old language:
> 2) The third-party website imposes reasonable internal controls to prevent the collection, retention, and use of cross-site tracking data. Reasonable internal controls may consist of, among other practices, data segregation, encryption, access control, and employee training.
>
> Example:
> Example Analytics collects data on behalf of first-party websites in a single database table that all employees have access to.
>
> Discussion:
> Example Analytics has not imposed reasonable internal controls.

Wainberg - Directionally, I like the approach, but I would propose revising it to make it cleaner.

* I prefer "reasonable controls" to "reasonable technical precautions," because it's broader, and could encompass both business controls and technical controls.
* As to what the controls are for, it's to prevent the mingling of data across parties, right?
* I don't know what a "form that renders them legally enforceable" by all of those parties will be, especially across jurisdictions. However, if a company publicly states that it adheres to DNT, and if there's a requirement in DNT for parties in this context to have "reasonable controls" then that's adequate for enforcement, isn't it? I don't disagree with the direction of this, just need to make it workable.
* To your issue about scope, the vendor needs to reserve some

independent uses, such as to operate, maintain and improve the
service, prevent fraud, etc. They also might disclose data in
aggregate form to market the service, or for research.

Here's a draft proposal:

When a vendor or service provider collects or uses [some data] on behalf of another party, that vendor or service provider stands in the same position as the party with regard to DNT if the vendor or service provider: 1) will use the data in non-aggregate form only on behalf of the party, and 2) takes reasonable measures to ensure 1. Whether measures are reasonable depends on particular circumstances, but may include business or technical controls such as [TBD].

Notes:

* "some data" is a placeholder for a yet to be defined scope of data to which DNT applies
* I broadened to any parties, not just 1st vs 3rd, so that, e.g., vendors of vendors will be covered (and also because I continue to doubt that the 1st vs 3rd distinction is useful.)
* I propose, for clarity, that we refer to this type of relationship as a "vendor" or "service provider" relationship. I think that's consistent with usage in the industry, so will be better understood.

ISSUE-170: Definition of and what/whether limitations around data append

http://www.w3.org/2011/tracking-protection/track/issues/170

Chris Pedigo Language:

http://www.w3.org/2011/tracking-protection/track/actions/229

Potential definition of Data Append: the act of adding new information acquired from a third party to information collected about a website visitor.

Use Cases: Current business practices that would qualify as a “data append” vary greatly in scope, utility and function. For example:

1) Firstparty.com partners with Nike. When a customer buys a Nike shoe, they get 6 months free of a health-related service on the firstparty.com. The customer must visit firstparty.com and enter a code to receive the service. When the customer visits Firstparty.com, they enter the code which firstparty.com matches up to the sale of the Nike shoe. The process of matching up a code with the offline sale would be considered a data append. With restrictions on data append, DNT:1 users would not be able to participate in promotional campaigns.

2) Firstparty.com has a large database of customers. Occasionally, they buy data from a third

party to clean up the database (purge bad email addresses, correct address information, etc). This would be considered a data append.

3) A user wants to create an account on Firstparty.com. They type in their address and firstparty.com uses a third party data provider to automatically fill-in the zip code. That would be a data append.

4) Firstparty.com sells flowers via business relationships with florists around the country. When the user visits the site, firstparty.com might use a third party that matches the user's IP address with the user's likely location within a metropolitan area. The location information is then used to customize the inventory available to that customer. This practice would also be a data append.

5) Firstparty.com might acquire data from a third party about the demographics and behavior of firstparty.com's users. The third party collected the data after users opted in. This would be considered a data append despite the fact that users opted in to the third party data collection.

Chris Pedigo, 4 Sep 2012, 19:57:56

ISSUE-154: Are First parties allowed to use data (either offline or online) from third parties

http://www.w3.org/2011/tracking-protection/track/issues/154

DAA Definition: (Uses the term agent for what the spec calls service provider and service provider as an internet access provider)

The actions of agents and other entities that similarly perform business operations of First Parties are treated as if they stand in the shoes of First Parties under these Principles and thus such actions are not included in Multi-Site Data.

H. Service Provider
For purposes of these Multi-Site Data limitations, an entity is a Service Provider to the extent that it collects and uses data from all or substantially all URLs traversed by a web browser across Web sites in the course of the entity's activities as a provider of Internet access service, a toolbar, an Internet browser, or comparable desktop application or client software and not for its other applications and activities.
Employers are not Service Providers with respect to data collected regarding employees in the employment context.

Global Considerations

http://www.w3.org/2011/tracking-protection/global-considerations.html#data-controller-and-processor

1.4 Data Controller and Processor

In essence there are three categories of entities, as discussed in European privacy parlance, that map onto the parties in the DNT debate:

1. The party who determines the purposes, conditions and means of the data processing will be the data controller
2. The party who processes data on behalf of the controller and a separate

   legal entity than the controller is the data processor. The data processor acts on behalf of the data controller. The relationship between both parties is bound by a legal contract.

3. Any other party who have no specific legitimacy or authorization in processing personal data is a third party as in the residual category of actors.

Multi-parties: there can be use-cases where a controller determines the purposes, conditions and means of the data processing jointly with others, the joint controllers must determine the respective responsibilities for compliance.

There is overlap with the technical terms used in our discussions. The outcome is:

1. 1st Party (Data Controller)
2. Service Provider (Data Processor), because of contractual relation to the Data Controller
3. 3rd Party (3rd Party)

For the EU, the outsourcing scenario is clearly regulated. In the current EU Directive 95/46/EC, but also in the suggested regulation reforming the data protection regime, an entity using or processing data is subject to data protection law. A First Party (EU: data controller) is an entity or multiple entities (EU: joint data controller) who determines the purposes, conditions and means of the data processing will be the data controller. A service provider (EU: data processor) is an entity with a legal contractual relation to the Data Controller. The Service Provider does determine the purposes, conditions and means of the data processing, but processes data on behalf of the controller. The data processor acts on behalf of the data controller and is a separate legal entity. An entity acting as a first party and contracting services of another party is responsible for the overall processing. A third party is an entity with no contractual relation to the Data Controller and no specific legitimacy or authorization in processing personal data. If the third party has own rights and privileges concerning the processing of the data collected by the first party, it isn't a data processor anymore and thus not covered by permitted uses. This third party is then considered as a second data controller with all duties attached to that status. As the pretensions of users are based on law, they apply to first and third party alike unless the third party acts as a mere data processor.

Article 29 Data Protection Working Party Opinion 1/2012 on the concepts of "controller" and "processor"

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf

“Therefore, two basic conditions for qualifying as processor are on the one hand being a separate legal entity with respect to the controller and on the other hand processing personal data on his behalf”

- “acting on behalf means serving someone else's interest and recalls the legal concept of “delegation”. In the case of data protection law, a processor is called to implement the instructions given by the controller at least with regard to the purpose of the processing and the essential elements of the means.”

“the Directive contains two provisions which are specifically addressed to the processor and which define in great detail his obligations with regard to confidentiality and security.

- Article 16 establishes that the processor himself, as well as any person acting under his authority who has access to personal data, must not process them except on instructions from the controller.

- Article 17 in relation to security of processing establishes the need for a contract or a binding legal act regulating the relations between data controller and data processor. This contract shall be in written form for evidence purpose and shall have a minimum content, stipulating in particular that the data processor shall act only on instructions from the controller and implement technical and organizational measures to adequately protect personal data. The contract should include a detailed enough description of the mandate of the processor.”

Related Issues:

Issue-10: What is a first party?

http://www.w3.org/2011/tracking-protection/track/issues/10

Issue-54: can first parties use declared data while in a 3rd party context

http://www.w3.org/2011/tracking-protection/track/issues/54

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

http://www.w3.org/2011/tracking-protection/track/issues/32

Thomas Proposed to close this issue for the following reasons:
* If cookie synching (the technique) is used for data sharing that is permissible in the context of accomplishing a permitted use, then that should be fine without specific text.
* If, on the other hand, cookie synching (the technique) was used to share data *outside* the scope of the permitted use, then that should be prohibited by the existing spec, without specific text.

Issue-60 Will a recipient know if it itself is a 1st or 3rd party?

http://www.w3.org/2011/tracking-protection/track/issues/60

http://www.w3.org/wiki/FirstThirdPartyDetection

Potentially ready for close:
http://lists.w3.org/Archives/Public/public-tracking/2012Apr/0129.html

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.

A "third party" is any party, in a specific network interaction, that cannot infer with high probability that the user knowingly and intentionally communicated with it.

ISSUE-181: Finalize language regarding multiple first parties

http://www.w3.org/2011/tracking-protection/track/issues/181

Rob Sherman’s Language:

http://lists.w3.org/Archives/Public/public-tracking/2012Nov/0075.html

This text reflects proposed text for Section 3.5.1.2.2, with a textual change that I received and adding language to clarify the status of "simple" web plugins. With this draft, I suggest that the status of ACTION-273 be changed to "pending review."

* * *

3.5.1.2.2 Multiple First Parties

For many websites, there will be only one party that the average user would expect to communicate with: the provider of the website the user has visited. But, for other websites, users may expect to communicate with more than one party. In these instances, a party will be deemed a first party on a particular website if it concludes that a user would reasonably expect to communicate with it using the website.

URIs, branding, the presence of privacy policies or other disclosures that specifically identify a party, and the extent to which a party provides meaningful content or functionality on the website, may contribute to, but are not necessarily determinative of, user perceptions about whether a website is provided by more than one party.

Example: Example Sports, a well-known sports league, collaborates with Example Streaming, a well-known streaming video website, to provide content on a sports-themed video streaming website. The website is prominently advertised and branded as being provided by both Example Sports and ExampleStreaming. An ordinary user who visits the website may recognize that it isoperated by both Example Sports and Example Streaming. Both Example Sports and Example Streaming are first parties.

Example: Example Sports has a dedicated page on a Example Social, a social networking website. The page is branded with both Example Sports' name and logo and Example Social's name and logo. Both Example Sports' name and Example Social's names appear in the URI for the page. When a user visits this dedicated page, both Example Sports and Example Social are first parties.

Example: Example Fan Club operates a sports fan website that posts articles about sports teams. Example Streaming provides an embeddable widget that allows the display of a video from a sports game. Example Fan Club embeds this widget at the bottom of one of its articles. The website does not identify Example Streaming in the URI, includes no Example Streaming branding, and does not refer to the Example Streaming privacy policy. The only functionality that Example Streaming provides on the website is the display of the video through its widget. Consistent with the standard described in section 3.5.1.2.1, Example Fan Club is a first party and Example Streaming is a third party.

Rob Sherman

ISSUE-184: 3rd party dependencies in 1st party content

http://www.w3.org/2011/tracking-protection/track/issues/184

As anyone that plays around with ad blockers, selective javascript tools, cookie killers and assorted privacy-enhancing browser extensions can attest there is a steady increase of content provided by what under the current text would be a 1st party that cannot be viewed unless content from a 3rd party is also accepted by the UA, be it cookies or javascript.

This raises an interesting situation if we have DNT. For example we have a 1st party that is trusted by the user and also claims to comply to DNT and a 3rd party that is neither. Since the 1st party content is technically dependent on 3rd party content, the user has the choice between either granting consent to the 3rd party in order to have the 1st party function properly or not getting the content at all.

To what extent is such consent informed, genuine and meaningful?