First Party

* Not too much debate on first parties
* One area without a resolution is appending 3rd party (offline) data
	+ Most don’t think its within the scope of tracking
	+ Maybe its not a good fit within DNT
	+ May be a privacy concern, but not a DNT issue
	+ DNT is ‘stateless’ technology discussing a specific transaction, this is beyond that
	+ Possible for any party to add additional rules based on jurisdiction; but DNT is the baseline rule
* Frank’s goal: not to restrict the usage of a DNT signal for a first party
	+ This is our goal, but it’s a may not a must
	+ Wewant to codify here the common ground
	+ First partys can choose to do more if they receive DNT:1
* First party cannot share (send) data with a 3rd party if that other party is not a first party or service provider
* Sending
	+ Cannot ‘send’
* First Party responsibility 1:
	+ If you receive DNT:1, you cannot facilitate sharing with a 3rd party for data profiling
* Can first parties enforce compliance for third parties on its site?
	+ There are other ways to protect data on its site
	+ Its impractical to ask first parties to police its 3rd parties
	+ DNT is a signal to me as a user to interact with that site
	+ Can’t feasibly bar first party to tell data to third party
* What are the obligations of a first party if they say they’re DNT complaint?
	+ The only obligation it has is to not facilitate third party tracking
	+ The first party has a really hard time telling third parties who’s on its site
	+ First party has no restrictions on receiving/using data for its own purpose
	+ Material difference between going to BlueKai to get data about them and getting data from a service provider like Acxiom
	+ First party gives data to 3rd party data vendor; cannot be used for any purpose other than getting data back from the vendor
	+ If the third party isn’t on the site, there is no way for it to ‘come back to the user’ with response headers
	+ Imagine I’m a website. I know their IP address because I get that. I can use a service to see if this IP address has been involved in any attacks. This service responds yes or no. Is that allowed?
		- It should be, but may need to be parked because it’s a use case we haven’t thought through yet
	+ FB: We should not prohibit first parties from sending the data to a 3rd party
		- It doesn’t care about how the user sends the data on to a 3rd party
* We NEED TO TAKE CARE OF PRODUCT FULFILLMENT USE CASE
* Would first parties store DNT flag within log files?
	+ Tat would require some significant infrastructure changes
	+ JC: This should be in the standard log files
	+ FB: The fact that I’m in seattle and sent a bunch of messages isn’t assocatiated with the DNT header
	+ JC: When I’m processing that one server log and see the DNT header, then I can record it
	+ FB: Because you’re a first party, there should be no prohibition on sharing
	+ Susan: What I’ve understood the requirement to be is that the first party cannot share the data with third parties to enhance/augment profiles
	+ Privacy advocates have said that its not enough to get consent by agreeing to Terms of Use/Privacy Policy
* Is ‘share’ button a consent mechanism?
	+ But, does that include whether I’m in seattle when I share it?
* DNT shouldn’t affect the first party’s broader ability to do business
* Maybe suggest to the group that being in a logged-in state may impact the application to DNT
* Question is: To what extent is it practical to restrict a first party from sharing data with third parties (who are not a service provider) when the first party receives a DNT:1 signal?
	+ What they are trying to get at is trying to create a work-around from having the third party on the site directly
* **A first party cannot subvert DNT by intentionally sending data to a third party that the third party would have received directly itself if it was present on the page itself**
	+ Cannot help a third party bypass the DNT signal
	+ Someone is going to have to audit against DNT whether that will have force
		- Priority should be simple and clear that users, sites, auditors can check it
		- Point of non-consensus, but am moving on
* DNT is flagged within the logs, and when the application is processing the logs, you look to see whether the use is affected by DNT. If so, honor it; if not, don’t honor it.
	+ In private discussions, regulators get that
	+ Don’t include that data within the permitted uses

Permitted Uses

* Add product fulfillment
* Fraud - needs to be broad
* Security - needs to be broad
* Transactional - needs to be broad
* Contextual serving
* Aggregate Reporting
* Analytics
	+ Some analytics – needs further clarification
* De-identified
* Legally required purposes
* Product debugging and improvement
* Service monitoring
* Hard part is ‘retention’
* Can’t limit all retention to 2 weeks
* Perhaps can use some technical and process rules to limit access to the data
* Whole argument for permitted uses is: you can’t keep the information that long otherwise it will be abused
	+ Instead, we should be addressing the abuse
	+ Have good standards for re-identification if it is retained
* People do not believe that we will limit access to use data appropriately
* Long-tail publishers need longer retention periods because they need it to retain diversity/known audiences. Cannot do it with 2 weeks of data. Got to have tools to sell inventory to advertisers
* “What’s protected depends a lot on who’s looking”
* Can’t make ‘absolute’ standards. Need to do it with reasonable protections and limitations
* In any of these, there needs to be a path for innovation.
* Market Research
* Define terms for which it means to put data in ‘databases’. There can be separate records for each permitted use
* “Access controls and technical mechanisms”
* Frequency capping (should be a broader category for which that falls) – maybe campaign management
	+ Needs to be spelled out further
* Making sure that two competing advertisers ads aren’t side by side/on the same page
	+ Can this be contextual advertising?
	+ **Content delivery management**
		- Conflicting advertisers
		- Advertisers don’t want to be on certain pages
* Reading the FTC’s accepted practices
* Characterize it as:

Third Party

 - when you’re a third party, you can’t write to a profile

Service Provider

* Under contract that prohibits the data for its own purpose except for permitted uses
* Contract needs to say that the services provided need to act on its behalf and have the same obligations

As part of a relationship with a 3rd party on its site, you ‘ask’ that it be compliant with the specs

* From the EU perspective, it’s the websites responsibility at the end, not the responsibility of the ad network
* To the extent that you have a relationship with the third party, ask that the third party be compliant

Small

Large

Small

large