Do Not Track

Nokia Browser Position

- Vikram Malaiya

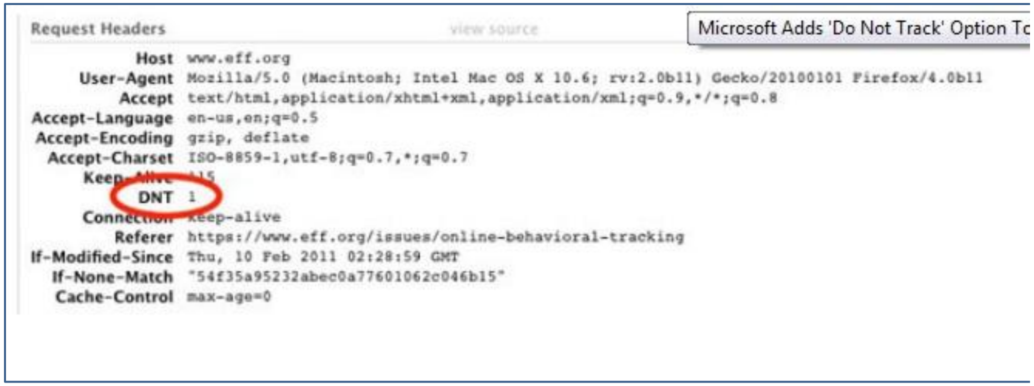
Our understanding of Do Not Track (DNT)

- DNT is a technology to enables users to opt out of third-party web tracking
- No agreed upon definition of DNT. There are currently 3 major technology proposals for responding to third-party privacy concern.
    1. Stanford University and Mozilla’s DNT HTTP Header technique.
    2. Blacklist based technique such as Microsoft’s ‘Tracking Protection’ which is part of IE9
    3. Network Advertising Initiative’s model of a per company opt-out cookie. Opt-out cookie approach is being promoted by Google.

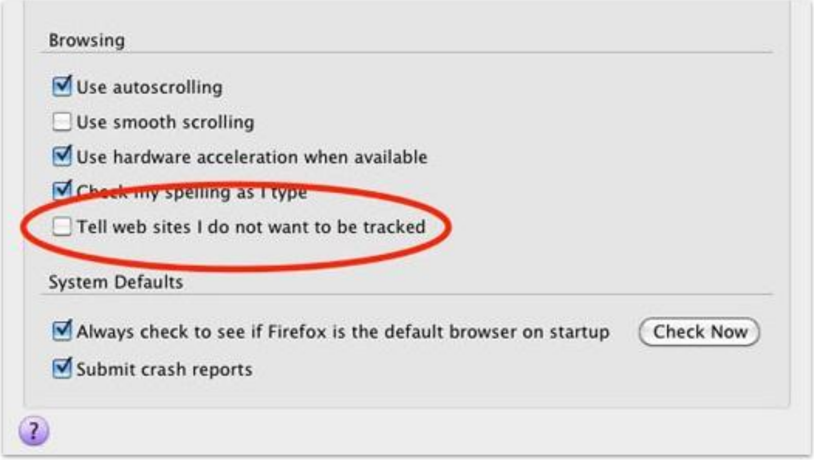
DNT as HTTP Header

The Browser adds ‘DNT’/ ‘X-Do-Not-Track’ to its http header. The header is sent out to the server with every web request. This header acts as a signal to the server suggesting that the user wishes to opt out of tracking.

Adoption: Firefox 4, IE9



```
             Host  www.eff.org
       User-Agent  Mozilla/5.0 (Macintosh; Intel Mac OS X 10.6; rv:2.0b11) Gecko/20100101 Firefox/4.0b11
           Accept  text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
  Accept-Language  en-us,en;q=0.5
  Accept-Encoding  gzip, deflate
   Accept-Charset  ISO-8859-1,utf-8;q=0.7,*;q=0.7
       Keep-Alive  115
              DNT  1
       Connection  keep-alive
          Referer  https://www.eff.org/issues/online-behavioral-tracking
If-Modified-Since  Thu, 10 Feb 2011 02:28:59 GMT
    If-None-Match  "54f35a95232abec0a77601062c046b15"
    Cache-Control  max-age=0
```



Browsing

☑ Use autoscrolling

□ Use smooth scrolling

☑ Use hardware acceleration when available

☑ Check my spelling as I type

□ Tell web sites I do not want to be tracked

System Defaults

☑ Always check to see if Firefox is the default browser on startup

☑ Submit crash reports

DNT as HTTP Header

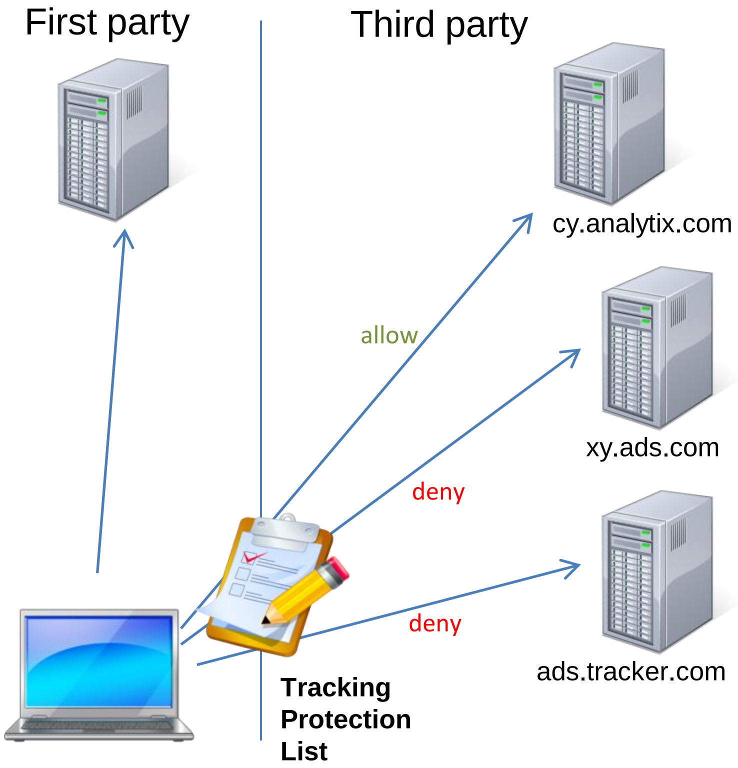
- Pros:
  - Scope: Server could apply restrictions to all third party entities and tracking mechanisms
  - Persistent: No reconfiguration needed once set
  - Simple: Easy to implement on the browser side
- Cons:
  - Only work as long as the server honors users preferences
  - No way to enforce national regulations/legislations to servers located beyond country boundaries

Block(Black) List / Tracking Protection

This is a consumer opt-in mechanism which blocks web connections from known tracking domains that are compiled on a list.

Adoption: 'Tracking Protection' in Internet Explorer 9

The downloadable Tracking Protection Lists enable IE9 consumers to control what third-party site content can track them when they're online.



Block(Black) List / Tracking Protection

- Pros:
  - More reliable than http header, because it put no reliance on trusting the server to honor user preferences, and it transcends national legal boundaries
  - Blocks third-party cookies, tracking pixels, web beacons, hit counters, analytics scripts, and other tools used for tracking.
  - Blocks ads as well (Pro/Con)
- Cons:
  - Only covers resources on the block list
  - Consumers have to judge the merit of a block list
  - Block lists need to be actively updated
  - Big players such as Google/Facebook not on the block list would still be able to track user behavior as a third party

Opt-Outs Cookie Approach

- An Icon based self-regulatory approach proposed by Network Advertising Initiative (NAI) in US, and by European advertising industry alliance(EASA) in EU
- The scheme does not depend on any special Browser setting, it works by adding an icon to behavioral ads served on websites to indicate it is a behavioral ad
- A click on the icon leads the user to www.youonlinechoices.com (EU), or www.aboutads.info (US). These websites allow users to opt out of behavioral advertising by selecting one or all advertisers that are listed as serving him behavioral ads
- The sites set a third party (opt-out) cookie on user's browser to capture's his choice. This cookie goes out to the advertisers in the subsequent browser sessions to indicate user's choice

Adoption: Google Chrome's Keep My Opt-Outs Extension, helps user maintain persistent opt-out cookie

Cookie Opt-Outs Approach

- Pros:
  - Driven by a industry driven self regulatory program

- Cons:
  - Lack of icon visibility, poor icon placement will render this approach ineffective
  - Persistence, not clear is the cookies could be accidently deleted
  - Narrowly focused on only online advertisements
  - Only covers the ~70 NAI members in US
  - No visibility into commitment of participating advertisers. Advertiser could choose to honor user's request based on their commitment/compliance to NAI/EASA's best practices recommendations

Position

- The HTTP header based DNT approach has merits because the simplicity and built in persistence in its design. However, given the cons mentioned in this report, this scheme alone may not be enough to protect online privacy, but it is a good step forward
- This scheme would complement the EU privacy directive that calls for “explicit consent” to be collected from Internet users who are being tracked via cookies. This directive comes in effect in May 2011
- We also support the self-regulatory opt-outs approach proposed by NAI and EASA, however this approach needs to resolve the open questions that we have posed in this paper to be effective. Moreover, such approach requires wider adoption by companies across Globe