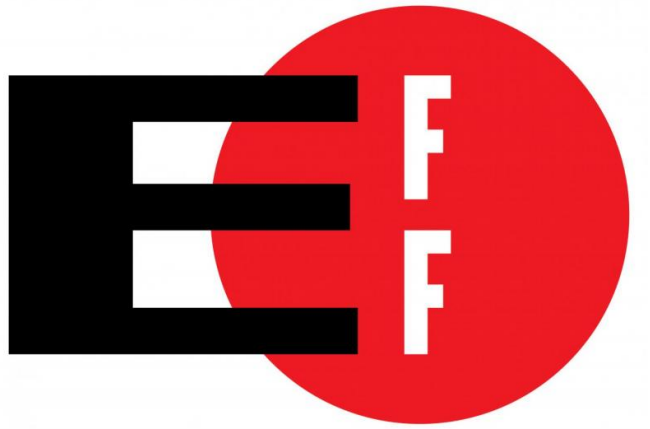
EFF and partners place Do Not Track on higher plane

5 August 2015, by Nancy Owano



Yes, you have the option of "Do Not Track" when using well-known browsers. Still, reports come in regularly of stealthy online tracking activities, where your reading histories can be exploited. An announcement this week from a coalition of companies along with the Electronic Frontier Foundation (EFF) seek a better route both for privacy-minded users as well as for advertisers.

The EFF, a privacy company called Disconnect, and the coalition of Internet companies are behind the push. They have issued a new policy standard for a stronger DNT setting to accommodate web browsing. They look toward a standard that, coupled with privacy software, can improve people's protection levels.

"Tracking by advertisers and other third parties is commonplace on the Web today, and typically occurs without the knowledge, permission, or consent of Internet users. You can see evidence of this when ads appear around the Web that are eerily based upon your past browsing habits; meanwhile, the underlying records and profiles of your online activity are distributed between a vast network of advertising exchanges, data brokers, and tracking companies," said the EFF news release.

One key point about the new standard effort is that it is not designed to kill advertisers' business. "The new DNT standard is not an ad- or tracker-blocker, but it works in tandem with these technologies," said the release. It's a policy that strikes a balance between user privacy and the needs of service operators.

Just consider "a viral surge in ad blocking, massive losses for Internet companies dependent on ad revenue, and increasingly malicious methods of tracking users and surfacing advertisements online," according to Disconnect CEO Casey Oppenheim, who hopes the approach can pave a better path that "allows privacy and advertising to coexist."

They also hope advertisers and data collection companies can be "incentivized" to respect a user's choice not to be tracked online. EFF Chief Computer Scientist Peter Eckersley commented that "These companies understand that clear and fair practices around analytics and advertising are essential not only for privacy but for the future of online commerce."

The EFF posted the DNT Policy as a text file; domains can post the words in verbatim form to commit to respecting a meaningful version of Do Not Track, in such a way that other software can tell they have done so.

"Whether their business is analytics, advertising, or social networking, companies dealing with data must be persuaded to respect a universal opt-out from tracking and collecting personal data without consent," said the EFF site. "Under our policy, compliant entities should not collect unique identifiers such as cookies, fingerprints, or

supercookies from DNT users, unless one of the exceptions below applies or the user has given her informed consent."

The policy document states: "This policy document allows an operator of a Fully Qualified Domain Name ('domain') to declare that it respects Do Not Track as a meaningful privacy opt-out of tracking, so that privacy-protecting software can better determine whether to block or anonymize communications with this domain."

Also, one of the requirements is about "end user identifiers." The document said, "If a DNT User has logged in to our service, all user identifiers, such as unique or nearly unique cookies, 'supercookies' and fingerprints are discarded as soon as the HTTP(S) response is issued. "

Why would a domain operator want to get involved in this? According to the EFF site, "A domain operator may choose to post this policy because it wants to meet best-practices privacy standards, and comply with user opt-outs from tracking. It may also comply because it wants to signal to privacy protection software (like Privacy Badger) that it respects Do Not Track, so that its third-party embeds are less likely to be blocked. In the former case a site may post the policy on most or all of the subdomains that it operates; in the latter case it is more likely to be posted on domains intended for third-party embedding only."

In the FAQ section, they point out that their policy is not intended to be compatible with businesses practices that involve the non-consensual collection of Internet users' reading habits or online activities. "It is a document intended to give users strong privacy protections, which means that in the current Web environment only some companies are going to be willing and able to post it."

Executive Editor at *BGR*, Zach Epstein, played it straight: "Advertisers stand to make big bucks by learning as much as possible about our browsing habits," he wrote on Tuesday, and though web visitors have the Do Not Track setting, some advertisers still track users nonetheless.

Epstein said, "the protectors of the Internet over at the Electronic Frontier Foundation have announced the creation of a new, more effective Do Not Track feature," and he also remarked that "The coalition's goal is not an unrealistic one—advertisers need to track users in order to serve relevant ads and increase revenue, and this won't change anytime soon. Users who specifically request to not be tracked, however, should not be tracked."

More information: EFF: www.eff.org/press/releases/coa … tandard-web-browsing