"Do not track" and beyond – Frank Wagner, Deutsche Telekom

"Do not track" is a developed Internet standard that enables users to indicate their own tracking[1] preferences to the websites they visit and the apps they use. Based on the European legal framework, users' opportunities for indicating their preferences are simplified.

Provided that the selection options are designed appropriately in the user agent, users can be "forced" to make a clear, intentional decision for or against tracking by prompting them to make a decision the first time the user agent is called.

This "decision" is made in the configuration of the user agent. The user only has to learn once where this setting is located and what it does. When opt-out scenarios are used, in contrast, users have to find out where the opt-out function is located, how to activate it, and how comprehensive it is anew for each individual website. Moreover, the fact that users are often forwarded to other websites to activate the opt-out function does not exactly give the impression that their interests are being followed.

In contrast to opt-out scenarios, where the website operators are clearly interested in having as few opt-outs as possible, the situation for opt-in scenarios is quite different. In this case, the website operators must assume major interest in opting in by the users. The corresponding mechanisms are positioned prominently; options for users to cancel a granted opt-in much less so.

In this context, "do not track" gives users much simpler options for indicating their tracking preferences. With "do not track", users no longer have to hunt through websites and apps to find the desired settings. As such, it would be consistent to make generic information about visited websites and used apps available to users at a centralized point. In this case, users would only have to learn once where to find this generic information for the respective website or app, similar to the do-not-track concept.

A minimal amount of generic information would be suitable for this purpose, but additional information can also be provided optionally. Options for extending this provided information for specific websites or apps should be provided.

Experiences from P3P should be utilized to identify the relevant information.

This implementation method would not only make it possible to address scenarios in conventional Internet portals; it would also be conceivable to use generic information to support decision-making in the business domain. This could involve cloud computing scenarios, however, in which personal data is processed. For SaaS (software as a service) offerings in public clouds, specific standardized criteria could be used to support decision-making. In this context, relevant factors for potential customers include where the data is saved, where it can be accessed, which sub-providers are involved in the production chain, which contractual foundation was selected between the contracting parties and which security levels are available. The possibility of positioning such information in a standardized place would be a major step toward improving the comparability of cloud services.

[1] Using "tracking" as a generally valid term in this paper requires that the term be defined and specified clearly and made transparent for Internet users. If it is not, it will not be possible to use a do-not-track function adequately.

We have to assume that the ability to compare similar offers would not only be relevant in the cloud computing domain, but could be transported to many other areas as well.

Therefore, now that "do not track" has created a standard for configuring user preferences, one objective of a future standard should be to improve transparency. The experiences from P3P should be taken into account accordingly.