Trackers Don’t Track People, People Track People
or What We Really Mean When We Say “Do Not Track”

A Position Paper from W3C Workshop on Web Tracking and User Privacy

Andy Kahl and Colin O’Malley - Evidon, Inc.

In 2003, Congress passed and then-presented George W. Bush signed into law the Do Not Call Implementation Act, which mandated that the Federal Trade Commission create and maintain the National Do Not Call Registry. It was an extremely popular measure, and why wouldn’t it be? Unsolicited marketing calls are categorically invasive. Adding a number to the registry means that, with few exceptions, unsolicited calls to that number are forbidden. It is a simple, analog decision and the legislation that allowed it was both timely and effective. At a glance, an initiative that would allow users to opt-out of online data collection seems very similar, and so proposals to limit or disallow these practices have earned the collective nickname “Do Not Track”. There is a natural tendency to also think of the solution in satisfyingly similar terms. Many of the proposed Do Not Track solutions, therefore, focus exclusively on the blocking or opting-out of data collection. While meaningful options of this nature are important components to an effective solution, they are not a solution in it totality. A privacy-conscious, ad-supported Internet requires transactional transparency, relevant information, and meaningful choices for the end-user.

Transparency is key on several levels - not the least of which to counteract the idea of creepiness that is often repeated in criticism of online data collection. In real-world transactions, shop owners learn your name, buying preferences, and other relevant details in order to customize your experience. Far from uncomfortable or “creepy”, this kind of service is heralded as attentive and valuable. If those same shopkeepers quietly looked at your other shopping bags to guess at your purchase history, shared what you bought with other stores, and used your driver’s license information to look up details about your family; you would quickly move from satisfied to disturbed. Anytime data that was not explicitly provided is explicitly used, there is a reflexive notion of privacy violation. The use of the data is not as problematic as the opaque nature of its collection. Transparent collection helps build a sense of trust and avoids giving users the creeps when that data is subsequently used. This is a general and systemic policy-based move, but one that is nonetheless critical.

The idea of transactional transparency is much more specific. This means notifying the user that data use or collection is part of a given user action. These actions could be page loads, ad delivery, widget execution, etc. This is a particularly important and inescapable feature of a robust and functional ecosystem, as users cannot build trust relationships with companies in the industry if they are not aware of when and how their data is used. It is noteworthy that many of the opt-out mechanisms discussed as part of Do Not Track proposals fall far short of the goal of transactional transparency. Technology that blocks as part of a list, obfuscated browser options, or by setting and maintaining opt-out cookies may offer the user a sense of control, but collectively lack a persistent indicator that the user has decisions to make. This could easily result in a false sense of privacy for end users, as data use and collection will continue in cases that the user isn't protected by an invisible list or opt-out cookie. That false sense of security is exacerbated when a one-click, Do Not Track mechanism exempts large categories of commercial entities, as many of the discussed proposals have. These exemptions are often warranted and reasonable; but without transparent and real-time notification, it is easy to envision a consumer believing that they have opted-out of whole types of tracking that are actually excluded from the Do Not Track feature.

It is, in essence, unreasonable to assume that an effective system can be created that does not include real-time, transparent user notification. To guarantee that users are well informed and are making active decisions about their data, users should be clearly notified every time data collection or use is attempted, even if they have previously opted-out. A solution without notification is particularly risky for publishers. An ideal system is one in which users decide if content on a given page valuable enough to allow for some data collection. Publishers, in turn, closely manage their partnerships with advertising companies to ensure that user data is only being used for this purpose. Without a system that standardizes transparent notification, users have no way to judge one site's data collection practices against another. Data collection becomes taboo instead of currency, and fundamental changes are required in the way online content is subsidized.

Transparent notification is only valuable when attached to relevant information. Simply displaying an icon that tells users "You've Been Tracked!" is not a legitimate aide to user privacy. They must have the opportunity to make informed choices. The informed nature of that choice is critical, which makes relevant information a core component of an effective solution. Data collection varies widely in both policy and practice. Companies differ on what data is collected, how that data is used, whether it is shared, how long it is stored, and to what extent the user can alter the data about themselves. The technology for data collection also varies widely, from server-side storage of elements like search strings to cookie-based session storage of a user's reaction to an advertisement, and many implementations in between. Some companies offer robust preference management where the user can shape the data collected. Even opt-out choices are variant, as an opt-out to one company doesn't mean the same as it does to another. Users need a real-time understanding of the companies involved in data collection on a given site, their policies, and then the choice to opt-out (coupled with an explanation of what that means). From a policy perspective, this information should be easy to understand and relevant to the actions taking place. It is critical that we learn lessons from previous failures in user notification like financial disclosures in user agreements from bank and credit card companies. Large dumps of standardized information anytime a user is notified of a data collection action undermines the value of transparency and does not allow for an informed decision by user. It's established that transparency is necessary in principle, and this transparency must be continued in practice through the provision of relevant, digestible, meaningful data.

A notified, informed user should then be allowed to make a meaningful choice. The data control offered by this choice should be clear, and the choice should be as close to permanent as possible. The core issue here is one of policy, not technology. It is certainly possible to release technology that uniformly blocks the common tools that data collection companies use to operate, but technological hurdles are easily circumvented, and cannot be regarded as a solution on their own. Data collection companies must adopt policies that result in a contractual understanding between their operation and consumers. Consumers must be offered a decision - and the must be given the opportunity to weigh the benefits of both sides of that decision. A permanently affixed “Not Me” sign is not a representation of an engaged, meaningful choice; and neither is a convoluted and token opt-out policy that offers consumers very little actual control. It is not outlandish to assume that this trade-off can be expressed in a way that allows a consumer to understand risk versus value, and subsequently make a material choice based on that understanding.

Collectively, these efforts can create an online ecosystem that is simultaneously advertising supported and privacy sensitive. Further, it supports a system of buyers and sellers, not creepy conspirators and their hapless victims. Informed, active consumers who understand the value of their data can leverage that currency in the same way they leverage their offline currency. The era of the friendly online shopkeeper is within our reach.

Author contact information:
Andy Kahl - andy@evidon.com
Colin O’Malley - colin@evidon.com
www.evidon.com