# Adobe Position Paper on Privacy and Tracking

**March 24, 2011**
**Submitted to the W3C in Anticipation of Participating in the**
**W3C Workshop on Web Tracking and User Privacy**
**By MeMe Jacobs Rasmussen, VP, Chief Privacy Officer**

## Introduction

Adobe believes that the W3C workshop on web privacy and tracking represents an important first step in an examination of a very complex and growing issue that affects all of the participants of the World Wide Web. Rarely has there been an issue such as this one, which touches all users (business, private, and government), all national and international governmental organizations, and all elements of commerce and industry (economic, legal, trade, and technology.) In part, this reflects the changing role of the World Wide Web, as well as signaling further complexities that will be encountered as the move to a massively connected world continues.

As a leader in online technology development, with a strong focus on the consumer experience, Adobe has a history of making the online experience enjoyable for consumers. As the owner of one of the largest online analytics businesses in the world, we understand the benefits of first party tracking, for first party uses, for the purpose of improving the online experience for consumers. We also believe that any interaction with consumers must be based on the principles of trust, mutual understanding, and integrity. We work to strike a proper balance – we understand that companies want to offer customers meaningful content and high-impact online interactions. Equally important, consumers want to experience the Internet in ways that speak to their unique interests. In every case, however, safeguarding consumer privacy is paramount.

## Summary of Adobe's Position

Adobe will support and participate in industry or standards initiatives that foster clear and meaningful choice regarding online tracking for purposes that are not obvious in context or commonly accepted, as described in the Federal Trade Commission's December 2010 Preliminary Staff Report. Adobe supports any discriminating "Do Not Track" mechanism that empowers, protects, and informs consumers that does not hamper innovation -- this is good for consumers and competition, and the many positive and necessary uses of data. These mechanisms should provide consumers with a clear understanding about the tracking to which they are opting-out.

The current *tracking* concern raised in the FTC's Preliminary Staff Report relates primarily to the use of information obtained by tracking a user's online activities for purposes that are not commonly accepted. The Report has a large focus on tracking for purposes of behaviorally targeting advertisements, but does not limit it to this use. Even the FTC, the consumer protection watchdog of the United States, does not take the position that all tracking violates a user's privacy. Rather, the Commission recognizes – properly – that it is the use of the information obtained by the tracking technology, taking into account users' reasonable expectations under the circumstances, that should be considered when determining whether privacy interests are implicated.

In its Preliminary Staff Report, the FTC took the position (albeit, preliminarily, pending its consideration of stakeholder comments) that *commonly accepted practices* do not require express consumer consent precisely because they are commonly accepted. Product fulfillment, fraud protection, and first party marketing are all listed within this category. So is the practice of websites collecting *information about visits and click-through rates to improve site navigation.* This falls within the preliminary set of commonly accepted practices because, just as offline retailers use consumer data to optimize their limited shelf space, websites need consumer data to optimize their sites. As such, the FTC does not believe this practice would require user consent. This form of tracking is distinguished, for example, from the unanticipated practice of selling personal information to third parties for secondary purposes unrelated to the purposes for which the data was originally collected. An industry standard solution geared towards protecting users from *unwanted tracking* should clearly define the specific type of tracking on which the solution focuses. [1]

Moving forward, we believe that "clear and meaningful choice" requires clear and meaningful definitions of the problem, its component parts, and its proposed solutions. Defining the problem requires understanding consumers' reasonable expectations. Only then can we determine where the tracking related solutions are required. Some of the current tracking proposals that have been announced by various browsers address many issues, some of which may not even pose threats to privacy. It is imperative that stakeholders define the problem we are trying to solve as a first step.

After the problem has been defined, the second step should be to reach a consensus on a clear set of definitions of the component parts of the problem. Without a clear set of definitions, we will continue to provide solutions that may or may not address real privacy issues and consumer

[1] The industry standard should also strive to satisfy the five requirements set out by the FTC: (1) a Do Not Track solution should be implemented universally, i.e. one-opt out that would apply to all sites that track; (2) the solution should be easy to find, easy to understand and easy to use; (3) the user's choice should be persistent, i.e. not deleted unless the user intended the deletion; (4) the solution should be effective and enforceable; and (5) the opt-out should apply to all defined tracking and relevant uses. As we discuss tracking – the problem and potential solutions – we need to keep in mind that the various initial solutions offered by the browser companies should gravitate to these five tenants or risk regulation.

concerns. More importantly, we risk doing harm to consumers' expectations and degrading the online experience for ordinary users. Just as privacy engenders trust, and therefore stimulates the continued growth of ecommerce, so does a positive, intuitive, engaging, and ever-improving consumer experience. Standards need to take into account both sets of reasonable end-user expectations and ensure that any solution retains equilibrium between the two. Tilting the balance too far in either direction does equal harm to the same objective: retaining an ecosystem that supports continued and increased trust and engagement online.

Adobe has a strong stake in personal privacy and user trust. Adobe's Omniture Business Unit is a leading provider of web analytic services that enables customers to capture, store, and analyze information generated by the use of their web sites to gain critical business insights into the performance and efficiency of their site, marketing and sales initiatives, and other business processes. Although the data generated by Adobe's products resides on Adobe's servers, each customer owns the data generated by the use of its site. By contract, Adobe has no right to access or use this data. In addition, Adobe does not allow use of the data for any purpose other than those of the owner (web publisher); that is, Adobe silos each customer's data for use by that customer.

Users benefit from this form of tracking. It enables streamlined paths through websites uniquely created by careful analysis of usage patterns and common needs and results in more engaging online experiences. Being able to bring the right information to the user at the right time benefits both the user and the business.

Another aspect of Adobe's business that is relevant to this discussion is its Flash technology platform. Local storage used by Flash Player (sometimes referred to as *Flash Cookies*) may be used to track users in place of cookies. It will be important for Adobe to understand the implementation of a Do Not Track solution to ensure that the user's choice is relayed to the Flash developer. It is not possible for Adobe to know how the local storage is being used by developers. It will be up to each developer to honor the user's tracking choice.

## Conclusion

Adobe fully supports measures to enable web users to have control over their privacy and their personal information. Adobe has a stake in finding suitable protections that empower consumers and build the foundations of trust that are necessary for ecommerce to continue to grow and thrive.

The ecosystem is complex. User expectations and assumptions are similarly complex. Any "fix" requires a clear articulation of the harm to be addressed and a solution narrowly tailored to address that harm. Simple solutions that prohibit all collection of data fail both prongs of this test. Assuming that all tracking is harmful, or even potentially so, is just as dangerous to the

ecosystem as assuming all tracking is benign. Addressing the assumption with a blunt instrument fails the narrowly-tailored test, and, by definition, risks collateral damage with no corresponding consumer benefit. Addressing all tracking with a single solution will confuse and frustrate users, perhaps even more so than they are frustrated now with no solution.

Adobe supports a discriminating Do Not Track solution that results from defining the problem from the perspective of consumers' expectations and defining key terms. Working together we need to identify the harm that must be addressed to foster trust and preserve the ecosystem without going so far as to cause frustration from unexpected and poor online experiences. We should focus on what consumers want and expect in terms of privacy and their online experience and tailor a solution that optimizes both.