Letter of Interest - W3C Workshop on Web Tracking and User Privacy

Ian Plunkett - Director of Eng. VizScore Inc.

April 26, 2011

Introduction

VizScore is an early stage startup in the email marketing space. Email marketing is most effective to the extent that data about individuals is collected as they leave information about themselves across the web - usually email addresses and often times more intimately identifiable details. Using these data to support marketing initiatives presents a number of unique challenges. Capturing information about browsing habits can be beneficial to consumers and marketers alike as it can enable increasingly relevant marketing communication. Marketers can present a more personalized experience that can lead to an increased ROI and consumers can be directed to products and services they are more likely to want. On the flipside, most consumers do not understand how and where data they have implicitly and explicitly provided are distributed across the web. This lack of understanding often leads to a general fear of data collection. A combination of education and technical standards will become increasingly important in maintaining a healthy balance that protects the identities of consumers on the web and allows for the best possible experience online.

Rising Influence of Real Identities across the Web

The rising notion that a user's online persona should be directly tied to their real life identity will complicate efforts to assuage concerns over tracking users across the web. To take an example from the fairly ubiquitous Facebook, we have "Like" buttons, Facebook Connect and Facebook Comments implemented across an ever-growing number of sites (Google and others have similar services.) Analyzing data produced by these widgets creates a fairly comprehensive user behavior profile. As these types of services gain traction, the user experience across the web becomes more and more reliant on personalized services. If the user chooses to opt out of such services, they will experience a degraded version of the web. Using HTTP headers to add "Do Not Track" features to websites will result in two-tiered systems. Many website developers may choose to entirely block visitors who enable such features because the development cost and subsequent ROI will not justify the effort. This makes initiatives to introduce code implementing "Do Not Track" features less attractive and will most likely hamper widespread adoption. Similarly, users that are not tech savvy may have difficulty even understanding the ramifications of allowing themselves to be tracked online and may prefer that things "just work."

Online Data Retention and Theft

Data theft presents a persistent problem for any repository of personally identifiable information. Recently, crackers were able to breach Epsilon, a leading email marketing company, and steal personally identifiable information on an unknown (presumably large) number of people. The attack against Epsilon is not an isolated incident and any organization that tracks users online should have comprehensive security policies to minimize the risk of data breaches. Companies and organizations collecting behavioral information should also have clearly outlined and publicly available policies that describe what type of information they retain on individuals. Further, they should provide a path for consumers to request that their data be removed from said systems.

Conclusion

Through a combination of consumer/user education and clear and open policies, we can align marketing interests and consumer privacy protection concerns. Behavioral tracking on the web can be beneficial to both consumers and marketers. The industry should strive to keep the public informed of how they protect personal data and how they use those data to enhance their marketing communications and user experience.