Software & Information Industry Association
1090 Vermont Ave NW Sixth Floor
Washington, DC 20005-4095
SIIA

W3C Workshop on Tracking and User Privacy
Comments of the Software & Information Industry Association (SIIA)
David LeDuc – March 25, 2011

SIIA is the principal trade association of the software and digital information industry. The more than 500 members of SIIA develop and market software and electronic content for the business, education and consumer markets.[1] SIIA's members are software companies and information service companies, including companies that both provide and rely on Internet advertising. As leaders in the global market for software and information products and services, our membership consists of some of the largest and oldest technology enterprises in the world, as well as many smaller and newer companies.

For over a decade, SIIA has worked with policymakers at the Federal and state levels in the United States, and also with policymakers in Europe, Canada and other regions, to examine the implications and operations of privacy and related laws. This has included work with the relevant Federal agencies implementing existing privacy and security regulations and policies, notably, the Federal Trade Commission's (FTC) approach on unfair and deceptive trade practices, as well as implementation of the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), and the Health IT Act.

SIIA appreciates ongoing efforts, both within the government and industry groups such as W3C, to assess the important issue regarding online privacy, behavioral advertising and web tracking. SIIA recognizes the critical objective of many policymakers and consumer interest groups to enable individuals with a simple way to opt out of the collection and use of data regarding their online browsing activities.

This has been done for some time, typically through the use of persistent cookies which would signal an individual's choices to various Internet actors. Opting out of an ad network in this fashion does not mean that the user will no longer receive ads. It means that the network will no longer deliver ads based upon the user's web site visits. [2]

[1] Our website can be found at: www.siia.net
[2] See the Network Advertising Initiative's opt out program at http://www.networkadvertising.org/managing/opt_out.asp

Tel: +1.202.289.7442
Fax: +1.202.289.7097
www.siia.net

SIIA strongly supports the balance between privacy and the free flow of information, as well as the balance between the need for consumer confidence and continued innovation on the Internet. In an era of rapidly changing technology and business models, SIIA strongly supports a privacy framework that is industry-led, voluntary and enforceable.

With respect to "tracking" and behavioral advertising, SIIA believes that efforts to provide consumers with a clear and easy opt-out should also be effectively focused on addressing potential harm, and they should be mindful not to undermine the benefits of online behavioral advertising. A recent study estimated that targeted ads generated almost three times the revenue of regular run of network ads and accounted for 18% of the total website ad revenue.[3] As many website publishers themselves have noted, restrictions on advertising through ad blocking would risk undermining their economic basis. [4] While SIIA doesn't oppose creation and use of ad blocking mechanisms, it is critical to recognize the economic harm that could come from confusion between ad blocking and tracing protection—to date there seems to be much confusion in this area, with many of the solutions being marketed as tracking protection that are largely ad blocking devices.

The W3C is a very useful form for assessing the various marketplace options provided and to ensure that private sector mechanisms are effective in promoting consumer choice and preserving the benefits of online behavioral advertising. SIIA is closely studying this issue and we have engaged our members in a dialogue to help private sector development of effective solutions. Following are some of our key conclusions to date:

- **Tracking must be clearly defined** – First, in order to have a productive discussion about online tracking, it is critical that the discussion be focused on the definition of tracking. Generally, "tracking" is not clearly defined. That is, tracking information has numerous potential uses other than targeted online behavioral advertising. Outside of any advertising context, many software and information companies use consumer data to deliver personalized services and to deliver content to users based on information they know about the user, such as improving search and better

[3] Network Advertising Initiative, Study Finds Behaviorally-Targeted Ads More Than Twice As Valuable, Twice As Effective As Non-Targeted Online Ads, March 24, 2010 available at http://www.networkadvertising.org/pdfs/NAI_Beales_Release.pdf. The study was done by Howard Beales, former director of the FTC's Bureau of Consumer Protection.

[4] See Ken Fischer, Why Ad Blocking is Devastating the Sites You Love, ArsTechnica, March 6, 2010 at http://arstechnica.com/business/news/2010/03/why-ad-blocking-is-devastating-to-the-sites-you-love.ars

tailoring applications and offerings to customers based on their preferences. It is often used for fraud prevention, risk management, control of spam and malware, intrusion prevention or detection.

Additionally, movement within a company's own website or suite of products is clearly not the kind of tracking that consumers are concerned about, and it is vital for businesses to track this kind of movement in order to optimize the performance and appeal of their websites. Similarly, websites routinely log the identity of the websites from which visitors arrive and to which they go when they leave. This provides valuable information about what attracts visitors to the site and what provides them with an incentive to leave. In a voluntary choice regime, these tracking activities would be permitted.[5]

- **Voluntary efforts are best suited to address the goals** – SIIA thinks that a mandated Do Not Track regime or a regulatory requirement to this effect would likely have harmful effects. Government-mandated anti-tracking mechanisms might short circuit the development of these valuable uses of tracking information. On the contrary, voluntary do not track initiatives would likely be better able to accommodate valuable uses while still allowing appropriate user control. SIIA is encouraged by many of the mechanisms under development by industry to inform and provide choice to consumers. SIIA is confident that voluntary choice mechanisms will sufficiently balance the needs of consumers, advertisers and content sites. The voluntary compliance by all Internet actors with the robots.txt protocol is a good example of how a voluntary system can produce desirable policy results without a government mandate.

- **Tracking Protection Lists (TPLs) present many undesirable outcomes** – First, the name is misleading. TPLs are focused not only on enabling users to block just tracking cookies, web beacons and other tools to track movements and activities on the web, but also block ads entirely.[6] The early providers of TPLs include the ad blocking services of EasyChoice, Privacy Protection and Abine.[7] Some users might want to

[5] Peter Eckersley makes many of these points in his commentary, "What Does the "Track" in Do Not Track Mean?" February 19, 2011 at https://www.eff.org/deeplinks/2011/02/what-does-track-do-not-track-mean
[6] Ed Bott, IE9 and Tracking Protection: Microsoft disrupts the online ad business, February 13, 2011 at http://www.zdnet.com/blog/bott/ie9-and-tracking-protection-microsoft-disrupts-the-online-ad-business/3004
[7] Ed Bott, Privacy protection and IE9: who can you trust? February 14, 2011 at http://www.zdnet.com/blog/bott/privacy-protection-and-ie9-who-can-you-trust/3014?pg=2

block ads in addition to blocking the tracking cookies, web beacons, and other devices that can track their movements from web site to web site. But it is not useful, and potentially harmful to the economic model of the Internet, for ad-blockers to be mislabeled as tracking protection solutions. There are technological solutions that can effectively prevent tracking and still allow for ad placement that isn't behaviorally targeted. It is these solutions and only these solutions that should be described as tracking protection. It is critical that discussions are clear on this point.

Further, there is a substantial possibility of consumer confusion regarding these lists. TPLs do not easily reveal the parties/domains blocked, so users may think they are blocking only bad actors, but in fact end up blocking sites that they actually want to see. In order for this to be implemented effectively, there is a high level of technical understanding necessary by the user. Even in such cases, accidental blocking is quite likely. Also, some TPLs allow third-party domains listed to be displayed. Other TPLs are exclusively blocking lists. When a user installs multiple lists, hierarchy rules provide that "allow instructions" trump "block instructions." This is inherently confusing to users and can create big problems.

- **From a technological and user experience perspective, SIIA would like to see continued support for voluntary opt-outs of tracking** – Persistent opt-out cookie initiatives have proven to be a highly effective mechanism for easy opt-out. Implemented as either a plug-in or a native component of browsers, this approach can provide a highly effective way for users to opt out of personalized advertising from participating networks and store the setting permanently. Importantly, the focus on the technological activity of "tracking," such as managing cookie controls, seems to be a highly effective approach, more so than approaches that simply shut off crucial parts of web pages and ultimately threaten to compromise user web experience.

- **The focus on browser web tracking is quite limited** – Less and less Internet activity is conducted through the browser and more is being done through applications such as instant messaging, voice over internet, RSS feeds, and streaming video. These applications use the Internet's underlying communications protocols, but they do not

use the browser capabilities.[8] By virtually all accounts, these trends represent the future of the Internet. Therefore, while a browser-based do not track mechanism is a useful endeavor, it is generally a narrow approach to the greater challenge of providing users with choice on "tracking." Again, in this broader effort, a voluntary initiative would be best suited to handle technological innovations and developments of this nature, and the W3C is a well-suited forum to discuss among key stakeholders.

[8] Chris Anderson and Michael Wolff, "The Web is Dead. Long Live the Internet," Wired, August 17, 2010 http://www.wired.com/magazine/2010/08/ff_webrip/all/1