Comments on Proposed Revision of the Policy On Web Tracking Technologies for Federal Web Sites (FR Document E9-17756)

U.S. Public Policy Council of the Association for Computing Machinery

August 10, 2009

On behalf of the U.S. Public Policy Council of the Association for Computing Machinery (USACM), we submit the following comments in response to OSTP's request for comments about web tracking technologies on Federal Government websites.

With over 94,000 members worldwide, the Association for Computing Machinery is an educational and scientific society focused on advancing computing as a science and a profession. USACM serves as the focal point for ACM interaction with U.S. government organizations, the computing community, and the public in all matters of U.S. public policy related to information technology. Should you have any questions or concerns, please contact Cameron Wilson at our Public Policy Office, 202-659-9711.

INTRODUCTION

We commend OSTP for recognizing the need to update federal government policies regarding the use of cookies by government websites. By providing customized experiences to individual users, or helping federal web developers understand usage patterns and information needs, cookies can significantly improve citizens' interactions with government websites and promote civic engagement.

It is important to broaden the discussion beyond the use of cookies because other web technologies (discussed herein) are also being used to track users' behavior—sometimes without their knowledge. If designed, developed, and implemented properly, web tracking technologies can provide a more personalized and effective user experience; thus, we believe a simple ban would be an overreach of policy, eliminating the advantages as well as the disadvantages of currently available web tracking technologies.

Our comments are derived from our experience with these technologies and application of the well-established standards of fair information practices.[1] USACM's Privacy Recommendations[2] provide a list of principles that seek to ensure minimization, consent, openness, access, accuracy, security and accountability for the collection and use of personal information. Regardless of how information is collected or stored, these general principles should be part of the design process for any website. All of these privacy recommendations are technically feasible.

---

[1] http://www3.ftc.gov/reports/privacy3/fairinfo.htm
[2] http://usacm.acm.org/usacm/Issues/Privacy.htm

Technologies

Three specific web tracking technologies are likely to be employed by the Federal Government: cookies, deep packet inspection, and web bugs.

There are various types of cookies, which can vary depending on the length of duration (session cookies versus persistent cookies) and on the underlying code used to generate the cookie (these include HTTP and Flash cookies). A session cookie allows a website to recognize a specific user as long as the user's browser remains open. These session cookies are useful for maintaining a user's online shopping cart through a series of product display scenes, leading to a final purchase, for example. When a session cookie does not specify an expiration date, it is deleted each time the user closes their browser.

Persistent cookies allow a website to repeatedly recognize the same computer on future visits until the cookie's expiration date. Persistent cookies provoke concerns about privacy because they enable web surfing to be tracked in ways that users may not understand or desire. In each case, code is downloaded from the visited website to the user's device. When cookies are purged after each web visit, the privacy and security concerns are much lower than when these cookies remain on a user's device after the web visit. Persistent cookies are an important feature in many or most systems for online behavioral targeting—a practice that is being actively scrutinized by the U.S. Federal Trade Commission.

Deep Packet Inspection (DPI) involves analyzing the data contained in each packet, rather than just the packet header. By deeply inspecting every packet an Internet user sends or receives, a complete and detailed behavioral profile can be constructed, typically to generate targeted advertising. In contrast to cookie-based approaches, customers have no way to easily "opt out" of DPI-based behavioral profiling. As such, it is considered by many to be a serious invasion of privacy. While the information provided by deep packet inspection might enhance the user's online experience, this technology is much more silent or invisible compared to HTTP cookies.

Web bugs are typically a single pixel matching the background color of the web page thereby appearing invisible to the Internet user. When the website is loaded, the advertising server can log the IP address of the HTTP request for the web bug so that it can track all the sites for which a particular IP address requests a web bug image. Web bugs are more limited than cookies because cookies can store actual personally identifiable information; however, Internet users are more easily able to block cookies.

New tracking technologies are invented from time to time, and government sites may want to consider using new technologies. Therefore, we recommend that any new policy not be limited to today's technologies, but be written to encompass tracking technologies generally.

Underlying Tensions

Web tracking technologies create underlying tensions; especially when personally identifiable information (PII) is used to tailor individuals' web interactions. Maintaining the privacy of this information may undercut the ability of a website to customize the individuals'

web interactions. This choice about whether to customize or not should ideally be up to the individual user. However, depending on the web technologies used, and the privacy and security procedures used by the website, this choice is often denied to the user.

At the same time, privacy concerns can possibly lead us too far in the opposite direction if they lead to preventing the use of web tracking technologies even for aggregated web analytics. Such analytics help monitor a site to determine if there are problems with attacks or other difficulties. Because it is possible for websites to use analytics without gathering PII, we believe the Federal Government should avoid using PII; otherwise, user notice and consent should be provided. The challenge is to ensure proper notice and consent as well as proper website design and access controls that can protect the information that is collected, used and stored.

In the following comments, we outline our recommendations for how to best strike this balance. These recommendations reflect the consensus of our USACM members.

RESPONSE TO THE CATEGORIES IN THE OSTP REQUEST

* The basic principles governing the use of such technologies;

In keeping with the privacy principles references above, unless a web tracking technology can be easily detected and managed by the user, it should not be part of the website design. This assumes that the user takes the necessary steps to manage the tracking technology on their computer(s), something no technology can guarantee. Tracking should be done openly and transparently. Until a newer, not yet envisioned technology is available, tracking across websites should be limited to HTTP cookies. Although many users are not aware of how to find, use, manage or remove HTTP cookies from their devices, browsers do give users greater visibility and control with cookies than with any alternative tracking method.

The general guidelines governing these technologies should not presume to know the type of device with which a user accesses a website. Accessing a website from a smart phone should not mean that a user receives less privacy than when accessing the website from a public computer or a home computer.

Government websites that embed third-party content (regardless of tier) need to ensure that those third parties cannot use personal information to track individuals absent explicit consent by the individual and disclosure of this third-party use of personal information to the individual and the government. The third parties that interact with government websites should be restricted to U.S. entities.

Any current or future secondary uses of the collected data should require a separate, additional notice to and consent from the user.

* The appropriate tiers;

The tiers, as currently structured, do not necessarily reflect levels of risk. For example, a tier one website, where single site visit information is collected, could link to other accounts or PII

during that visit. This would result in a risk of exposure even though that website may not store information beyond that visit. Each specific proposed use of web tracking technologies should be informed by a risk analysis that accounts for relevant context, including information sensitivity (e.g., information viewed on specific diseases might be considered more sensitive than information viewed on national parks).

All things being equal, however, we recommend that the level of privacy protections increase with each tier.

* The acceptable use and restrictions of each tier;

The language in the third tier—"purposes beyond what is needed for web analytics"—needs clarification. If those purposes include collecting information that could identify/locate a specific individual and/or create a personal profile, this should be explicitly stated in the notice and consent procedures for this tier. Any use for personalization should comply with fair information practices and should be restricted to the third tier. Any data collected for third tier uses should be carefully controlled in terms of access and use, and the notice required should be clear and conspicuous.

Cookies with data that contain or imply personally identifiable information (PII) should be protected by encryption or by a keyed hash so that the sensitive contents are not readable off-site. This helps ensure that cookies cannot be forged to gain access to PII, and if intercepted or scraped they are unlikely to provide any usable information. Including plaintext comments that describe what the encrypted/hashed field represents would allow the user to still see the cookie contents.

Collecting personally identifiable information may be necessary in the regular course of business with government, but it is unclear why such information would need to be collected in cookies or other web tracking technologies. A Privacy Impact Assessment (PIA) may help identify and rectify instances of unnecessary privacy risks by minimizing and/or eliminating the collection of PII.

If third tier collection and use take place on websites that contain or link to sensitive personal information, (financial, medical, legal, etc.), the importance of following fair information practices, including ensuring proper security and access controls, is heightened. Whereas the breach of personally identifiable information in general exposes individuals to undue and unnecessary risk, links to particularly sensitive information such as a medical condition or financial account information dramatically increase the risk and consequences of identity fraud or theft, along with the potential for other offenses or embarrassment.

* The degree of clear and conspicuous notice on each website that web tracking technologies are being used;

We recommend that websites employing web tracking technologies include a human readable short notice in addition to a machine-readable web tracking technology policy on their sites. This notice could be as part of or separate from the website's other privacy policies. This

information should be presented in clear and concise language formatted for easy readability. Should cross-tracking activity follow a person from a lower tier site to a higher tier site, the protections accorded the collected data should rise to the level of the highest-tier site visited. We recommend that the websites (and their privacy policies) be designed to display their tier and to recognize the tiers of other sites that might collect information from them.

* The applicability and scope of such a framework on Federal agency use of third-party applications or websites;

Given the potential for third parties to utilize the information collected via their applications or websites in combination with material they may collect from other sites, it is critical that any information collection about government website users by a third party undergo additional scrutiny. This scrutiny should apply to these third parties and their standards for the websites and developed applications. The objective here is to reduce the possibility of exposing PII through the third party, a possibility that would not occur if the data remained on the government website or system.

* The choice between an opt-in versus opt-out approach for users;

Ideally, users should have to opt-in to any collection and use of their personal information. That said, some common standards for identifying and managing cookies that the user deems worthwhile to keep would be helpful in making it easier for users to work with these technologies. Should a system utilize opt-out cookies, a means is needed to enable such cookies to be persistent. Currently, when cookies are deleted during periodic cookie management, or the regular scans of anti-spyware software, the opt-out cookie is lost—often without the users' knowledge. This issue can be addressed by creating a single, standard, government-wide opt-out cookie, and encouraging private-sector opt-out tools to support it.

* Unintended or non-obvious privacy implications; and

Given the unintended consequences inherent in many web tracking technologies, we recommend minimizing their use on Federal Government websites. We especially recommend avoiding or minimizing the use of tracking technologies other than HTTP cookies.

* Any other general comments with respect to this issue."

The security and privacy indicators of websites should be made compliant with the Americans with Disabilities Act (ADA). Some technologies currently in use by government websites, such as Flash, are non-compliant with the ADA. Research is needed to find solutions that will make websites more accessible to individuals of any capacity.

By taking steps to protect the privacy of personal information used on websites, the security of these websites will improve as well. It is a myth that privacy and security must be pitted against each other. By restricting the collection and sharing of information, especially where third parties are concerned, the government can reduce the threat exposure to its websites and systems, as well as to the websites and systems of the third parties and vendors that interact with those

government systems. Additionally, by minimizing the collection, use and storage of PII, associated security and compliance costs will decrease.