Both Hands in the Cookie Jar

by Alissa Cooper [1] August 17, 2009

The federal government has recently announced [2] its intention to revise the current policy governing how federal agency web sites use cookies and other tracking technologies on the web. This is a really significant development for those interested in technology, open government, and privacy, because it has the potential to change the way that federal agencies interact with citizens online. It's so important that we'd like to demystify some of the rumors floating around out there about the current policy, the new policy, and what it all means for privacy. First things first: the government already has a policy governing how federal web sites can use cookies and other persistent tracking technologies. As established in 2000 (and updated in 2003 -- see our previous post [3] for a brief history), the policy prohibits federal agencies from using persistent tracking technologies unless there's a compelling need, that usage is disclosed, and the agency head (or a delegate) personally approves that use. While that last provision about agency head approval may have stymied many agencies' efforts to use cookies, that doesn't mean there is currently an outright ban on cookie use. There isn't. Today, if an agency head wanted to approve the use of cookies to track and record intimate details about how citizens engage with the agency's site, the current policy would not stand in the way. And in fact, that's one of the main reasons why we think the cookie policy needs to be revisited. The current policy doesn't discriminate between different uses of cookies - it affords the same protections (compelling need, disclosure, and agency head approval) regardless of how an agency intends to use tracking technologies or what the potential privacy implications are. A better approach would (1) require a baseline set of protections for all uses that goes beyond what is in the policy today, (2) build in more robust protections for more privacy-invasive uses, and (3) leverage the expertise of the privacy office within each agency to determine which uses are appropriate. Luckily, the framework for revision that OMB has initially proposed [4] begins to go down that very path. OMB released a set of general principles to govern all federal agency uses of web tracking technology and a multi-tiered system that would accrue additional privacy protection to particular uses based on their potential privacy impact. While OMB is off to a good start, there's a lot of work left to be done to craft a policy that maintains the current policy's level of privacy protection while giving federal agencies the flexibility to employ state-of-the-art web technologies. In comments [5] that we submitted to OMB jointly with EFF, we provided detailed suggestions about how the new policy should work, including:

- Making sure the policy applies to all web tracking technologies (like web beacons, Flash cookies, DOM storage and the like), and not just cookies; - Requiring that agencies provide detailed disclosures about their web tracking intentions in the form of a Privacy Impact Assessment (PIA) that must be verified by the agency privacy office prior to deploying a tracking technology; - Requiring that agencies retain tracking data only as long as necessary for the purpose for which it was collected, and deleting certain information (such as IP addresses) immediately; - Requiring agencies to display an easy-to-use choice mechanism on every page of each site where cookies are used for analytics; - Differentiating between cookies used to store preferences (like the user's preferred language) and cookies used to store authentication information (which allow users to login and maintain a persistent identity); and - Requiring enhanced security, access, and consent procedures when authentication cookies are used.

The administration has pledged to make the government more transparent, open and participatory. Federal agency web sites are a key part of that strategy, but they've been limited in their ability to take advantage of all the advances in web technology that we've seen in the decade since the federal policy on tracking technologies was put in place. We now have the opportunity to fix the current policy, maintain its high level of privacy protection, and enhance the capacity of federal agencies to serve citizens online.

- security
- tbp
- Website
- •
- privacy
- <u>omb</u>
- CDT
- cookie
- Electronic Frontier Foundation
- IP address
- Adobe Flash

The yaring her that some the substantive changes and clearly give us credit. Details.

Source URL: https://www.cdt.org/blogs/alissa-cooper/both-hands-cookie-jar

Links:

- [1] https://www.cdt.org/personnel/alissa-cooper
- [2] http://blog.ostp.gov/2009/06/16/enhancing-online-citizen-participation-through-policy/
- [3] http://blog.cdt.org/2009/01/08/a-new-cookie-policy-for-egov-20-%E2%80%93-part-i/
- [4] http://blog.ostp.gov/2009/07/24/cookiepolicy/
- [5] http://www.cdt.org/privacy/20090810_omb_cookies.pdf