

## A New Cookie Policy for eGov 2.0 - Part I

January 8, 2009

The Obama Administration's promise to increase citizen participation in government using Web 2.0 technologies is already raising questions; current federal policies may need to change in order to take full advantage of such technologies. Challenges to successful use of these technologies will, no doubt, come from a variety of places: legal, policy, security and privacy. Ingrained institutional resistance is also a potential roadblock to innovative use of new technologies. One clear area of conflict is the federal government's policy on the use of state management tools, such as cookies. Many Web 2.0 services depend on remembering some amount of information about an individual. On the Web, the main way to remember visitors is by giving each a unique ID number. These numbers are stored in different ways, but usually they are stored in a file called a cookie. Because of agency privacy rules, and the fact that cookies are often used to track users, federal policy makes it very hard (almost impossible) to use cookies and other user tracking technology. As a quasi-governmental entity, President-elect Obama's **Change.gov** team has some space to try new ideas and techniques, and yes, use persistent cookies; however, the continued use of these tracking techniques after Obama is sworn will require a policy change or direct approval from the President himself. This will have to happen even if users give their permission, with complicit understanding, to being tracked through use of an ID number. Bottom line: federal cookie policy needs to be modernized by allowing government web sites to set cookies and give users the choice to accept or reject the technology. *The federal government should maintain a policy that guides agencies in the use of tracking technologies, but parts of the current policy need to be revised in order to better reflect the realities of agency culture, of user expectations, and technological progress. In addition, these guidelines should reflect [fair information practices](#) [1] in allowing users to make choices about the information that is collected when they visit federal websites.* **History Lesson** A bit of history - The [federal cookie policy](#) [2] was written in 2000, after the Office of National Drug Control Policy (ONDCP) contracted with DoubleClick to [use cookies to track users](#) [3] as part of an advertising campaign (remember that ONDCP also supports anonymous drug education and treatment). In response to criticism at this tracking of users on a government website, the Office of Management and Budget (OMB) [released a policy on the use of cookies](#) [4], explicitly stating a presumption that federal websites would not use cookies and laying out policies when cookie use was deemed necessary. This policy made it hard, but not impossible, to use cookies on federal websites. In 2003, the [E-Government Act privacy implementation](#) [5] policy expanded the types of technologies included under these policies to include any tracking technology that lasted longer than a user's one-time visit to the website. Currently, in order to comply with the federal cookie guidelines, a government website:

- must have a compelling need to gather the data through cookies;
- must provide users a clear and conspicuous notice of the use of cookies;
- must have a clear privacy policy explaining the collection of information through cookies and privacy safeguards for handling that information;

and must have personal approval from the agency head, or a delegate who reports directly to them. These policies gave federal websites better guidance on what kinds of technologies they were free to use, and what technologies needed further consideration. However, it is still not completely clear what kinds of technologies are covered by these policies, other than cookies or Web beacons, when they are not explicitly used for tracking. Additionally, these guidelines do not allow for user control at all; rather than allowing users the option of advanced features that are powered by cookies or tracking technologies, the policies mean no users have access to advanced features. **Problem With Policy: No User Control** In the years since these cookie policies were written, there have been [many enterprising stories](#) [6] on federal websites using cookies outside the OMB policy- most amusingly, [NSA](#) [7] and the [White House](#) [8] itself. This was not too surprising considering that many off-the-shelf products set cookies by default, but it did raise the issue again and again making it clear that there remains public concern over how tracking is done and whether the government can follow its own privacy policies. Since OMB issued these cookie policies, the use of persistent identifiers on the Internet has changed significantly. It may be time to re-evaluate acceptable uses

for cookies on federal websites. Many Web sites offer pro-active controls to allow, but not force, users to store information about themselves. Most Internet users have also come to expect the kinds of features and services from websites that are often dependent on state mechanism of some sort. *The problem is not that there is a cookie policy in place, it is that the current cookie policy does not provide user controls. Instead, we should allow federal websites to use modern technologies while giving meaningful privacy choices to the users of these websites. Modernizing these policies will let the government use Web 2.0 and continue exploring the kinds of innovative uses of the Internet developed through the campaign and the transition.* Tomorrow, we will explore we think a new policy should look like in more detail.

The copyright © 2003 by Center for Democracy & Technology. CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. [Details.](#)

**Source URL:** <https://www.cdt.org/blogs/ari-schwartz/new-cookie-policy-egov-20-part-i>

### Links:

- [1] <http://www.cdt.org/privacy/guide/basic/generic.php>
- [2] <http://www.whitehouse.gov/omb/memoranda/m00-13.html>
- [3] <http://shns.scripps.com/shns/story.cfm?pk=COOKIES-06-20-00&cat=AN>
- [4] <http://query.nytimes.com/gst/fullpage.html?res=9E07E2DC1E31F931A15755C0A9669C8B63>
- [5] <http://www.whitehouse.gov/omb/memoranda/m03-22.html>
- [6] [http://news.cnet.com/2100-1028\\_3-6018702.html](http://news.cnet.com/2100-1028_3-6018702.html)
- [7] <http://www.nytimes.com/2005/12/29/national/29cookies.html?ex=1293512400&en=1a7909602afc9cdb&ei=5090&partner=rssuserland&emc=rss>
- [8] <http://www.wired.com/techbiz/media/news/2005/12/69945>