New Federal Web 2.0 Rules Lack Full Privacy Protections

June 25, 2010

OMB today released two long-awaited memos on federal agency use of cookies and Web 2.0 services. As the Administration urges agencies to use new tools that make government services easier to use, it's reasonable that they re-evaluate the policies that also hinder the use of some of these tools. Most of the public have come to expect that pages will, at their request, make their interactions easier by remembering their preferences, and improving their website based on measurement tools like analytics.

Existing cookie and third party policies boils down to "don't use them." The government eased up in a memo [1] that came out with the Open Government Directive, clarifying that social media use typically doesn't fall under the Paperwork Reduction Act - but the memo did not address the privacy concerns that come along with using third party services or tracking users of federal websites. Open Government Day (as it was called by some) also did not include the memo revising the cookie policy that some were hoping for, but the memos on third-party services and measurement tool policies (i.e., cookies) have been released.

Luckily for web managers, the memos released today make it easier to use third party services, measurement and analytics tools, and customization for users. However, some of the guidance does not clearly require agenices to protect user privacy in ways we had hoped.

Agencies Using Third-Party Websites and Services

The first memo [2] - “Guidance for Agency Use of Third Party Websites and Applications” - addresses agency use of third party services, and how to protect privacy even as agencies interact with the public on sites that they do not have full control over. These technologies are often used in support of the Open Government Initiative, but the privacy implications and requirements had not been clearly set out for web managers. Using third party services makes it much easier to engage with the public, but pose privacy questions that have not been well addressed.

While the memo only addresses the use of third-party services toward the principles of the Open Government Directive, it seems that the memo should also guide agency use of all third party services on websites, including third party measurement or customization tools (which are not specifically addressed in the second memo).

A few important principles are codified in the memo, including that the public should always be able to get the same kinds of information at the agency website as they can on a third party website, and should never be required to use a third party site or service to engage with the agency. While these third party tools may be helpful and allow agencies to go where the public already interacts, they should never be the only way that a member of the public can choose to interact with the agency - and the agency should make it clear to the visitor when they move from an agency-controlled website to one that is maintained by a third party.

While the memo makes it easier for agencies to use third party services, it also lays out the requirements for using these services, including a Privacy Impact Assessment and prominent public notice to users of third party sites that while they may be interacting with government, they are doing so on a third party site.

When federal web managers listed [3] the barriers to using social media and other third party services in government, privacy was a prominent barrier in their use. This memo clarifies how, and when, to use third party services for openness in government - with an emphasis on ensuring that the public is informed how and when their privacy could be impacted. While agencies have already been using these third party services, guidance from OMB will ensure that there are consistent

expectations on the use of these services across agencies, and easily accessible public notices around privacy and use of these websites.

The New Cookie Policy

Addressing a more specific set of topics, today's second memo [4] – "Guidance for Agency Use of Third-Party Websites and Applications" – gives an update on the oft-maligned "cookie policy [5]" (which addressed all manner of tracking technologies online, not just cookies). This policy was a barrier to improving agency websites, but there was not a clear way to update the policy to enhance user control while allowing agencies more tools online.

When we offered suggestions for a new policy around cookies and Web 2.0 services for the government, we highlighted [6] principles to protect privacy while allowing agencies to use technologies available to measure and improve the user experience. Several of them are reflected in the new memos, but some are missing and the memo as a whole lacks the details we were hoping to see. While the use of measurement technologies (otherwise known as analytics) and website customization could be very useful for agencies, collecting information about visitors must be done carefully in order to ensure that privacy continues to be a paramount consideration on Federal websites.
Several of the cookie policy updates are vague or downright confusing. For example, the memo prohibits agencies from tracking "individual-level online activity outside of the website or application from which the technology originates." This may be aimed at addressing the case where government agencies act as third-party data collectors on other websites, but that is not at all clear from the text. Furthermore, if that is the aim of this prohibition, its existence serves to highlight the fact that the memo makes no distinction between first-party tracking and third-party tracking on government websites themselves. In our recommendations, we stated a strong preference for the use of first-party technologies and strict limits in cases where third-party technologies proved necessary. The memo fails to address the first party vs. third party question altogether.

OMB lays out several options for how agencies might provide users with choices about their participation in measurement and customization. Among these is a "client-side opt-out," otherwise known as agencies providing users with an explanation of how to block cookies in their browsers. This is an entirely inadequate policy for OMB to be promoting, particularly when the explanation linked from the memo recommends disabling all first-party cookies (whereas a clear opt-out process would opt users out of only those tracking technologies employed by government agencies). A large majority of commercial websites rely on first-party cookies in order to function properly. Many of these sites instruct users to turn first-party cookies on if they are off. Thus, users who follow the guidance suggested by OMB will likely end up with no privacy protection at all. A more protective policy would have required agencies conducting measurement or customization on an opt-out model to provided targeted, highly-visible opt-out mechanisms.

We are pleased to see the memo tackle the issues of data retention and access limits, particularly the requirement that agencies "may retain data collected from web measurement and customization technologies for only as long as necessary to achieve the specific objective for which it was collected." Unfortunately, OMB undercuts this requirement by suggesting that data can be retained for one year. This policy may be a result of a separate records management requirement for the federal government, but in any event it would have been helpful for OMB to more thoroughly discuss the relationship between records management and data retention for measurement and customization, rather than leaving interpretation up to the agency.

Despite these shortcomings, this memo is an improvement to the policies that agencies have had to work with until now. The memo makes it simpler to use cookies and other measurement technologies; where agencies were previously required to get agency head approval for the use of a tracking technology, the new policy is more targeted, requiring review by the Senior Agency Official for Privacy, as long as the technology does not track personally identifiable information. The memo does well to emphasize the need to inform users about their options and choose tools that provide simple and robust opt-out options, and the need for technical and policy restrictions to compliment each other in order to create privacy protective sites that also empower users and web managers.

Enabling the use of new technologies in government

As agencies push forward in using third party services and new technologies to enhance their sites, it is key to ensure that privacy is protected. All the enthusiasm in the world can't be put to good use if users don't trust agency websites to use these tools judiciously. We are also hoping that new tools from industry - easier opt-outs and privacy controls - will help users to make informed choices easily when interacting with government. The memos released today are a start towards a more nuanced way to approach these tools for federal agencies, but do not provide the guidance around measurement technologies that we hoped for.

CDT's Alissa Cooper also contributed to this piece.

- Web 2.0
- privacy
- Open Government

Links:
[1] http://www.whitehouse.gov/omb/assets/inforeg/SocialMediaGuidance_04072010.pdf
[2] http://www.whitehouse.gov/omb/assets/memoranda_2010/m10-23.pdf
[3] http://www.usa.gov/webcontent/documents/SocialMediaFed%20Govt_BarriersPotentialSolutions.pdf
[4] http:// Heather West 2:36 http://www.whitehouse.gov/omb/assets/memoranda_2010/m10-22.pdf
[5] http:// Heather West 1:53 http://www.whitehouse.gov/omb/memoranda_m03-22/
[6] http://www.cdt.org/policy/using-analytics-privacy-protective-way-government-web-sites-cdt-recommendations