




X CLOSE
OR ESC KEY



You are exiting the White House Web Server
Thank you for visiting our site.

You will now access
<http://www.facebook.com/whitehouse>

We hope your visit was informative and enjoyable.
To comment on the site, send feedback to the Web Development Team by [clicking here](#).

Six New Media Challenges

Legal and Policy Considerations for Federal Use
of Web 2.0 Technology

Peter Swire May 2009

Center for American Progress



Six New Media Challenges

Legal and Policy Considerations for Federal Use
of Web 2.0 Technology

Peter Swire May 2009

Executive summary

The Obama campaign set a new model for how to spread information through new media and social networking technologies such as YouTube, Facebook, Twitter, and others. It also sparked imagination about how these Web 2.0 technologies could usher in a new era of government transparency and citizen participation.

The Obama administration has already begun to take up some of the same technologies it used during the campaign and on change.gov. But it hasn't yet used these applications to the same extent it did previously, and that's largely because it is now subject to federal laws and regulations regarding privacy, disability access, advertising, and other issues.

This paper addresses six key legal and policy issues that the Obama administration will have to address for WhiteHouse.gov and federal agency websites to use Web 2.0 widely and effectively.

1. Privacy: Perhaps the most important privacy concern is current guidance that limits the use of persistent cookies on federal websites, even though such cookies are a standard feature of many Web 2.0 applications. The new administration will need to decide whether to alter that guidance, and it will face the related question of what privacy protections should apply when the federal government uses applications that send users to private-sector websites.

2. Access for those with disabilities: Section 508 of the Rehabilitation Act provides guidelines for making federal websites accessible to people with disabilities, including the visually and hearing impaired. All federal websites must be Section 508 compliant, but many Web 2.0 applications are not.

3. Commercial endorsement and advertising: Current regulations prohibit government websites from commercially endorsing any product or service, and also ban advertising. Use of any one Web 2.0 service over another could be considered an endorsement, particularly if it involves including a company's logo on a government website. And there could be reasons not to link to sites that include inappropriate advertising content.

4. Terms of service agreements: Federal employees and agencies are not allowed to accept any indemnification agreements, and most website terms of service use state, rather than federal, law to resolve legal disputes. No part of the federal government can therefore enter into a terms of service agreement unless it is modified to meet federal regulations.

5. The Paperwork Reduction Act and public records requirements: The PRA requires agencies to submit formal requests to the Office of Management and Budget before collecting information from the public. This does not appear to apply to user comments as long as federal websites do not require users to submit any information beyond personal identification, but will be an issue if the executive branch wants to collect any more specific information or conduct surveys. Federal agencies also need to comply with public records requirements, including the Presidential Records Act.

6. Security concerns and agency restrictions on staff Internet use: Many federal agencies block their employees from accessing social media websites and chat services, especially out of concern for computer security. These policies could essentially prohibit employees from working on Web 2.0 applications.

Many of the key issues posed by Web 2.0 technologies are legally similar. The federal government has obligations for what is done on its own websites. Those obligations do not apply when a user leaves the federal website and begins using a third-party service. Federal websites must be Section 508 compliant, for example, but as long as the federal website makes it clear to users when they are leaving for an outside website, that outside site does not have to be Section 508 compliant. The same applies for advertising and privacy issues.

Yet some significant federal policies are at stake when users leave a federal website. The federal government should not encourage the use of non-accessible web technologies, invasions of privacy, loss of security, or unreasonable commercial endorsements or advertising—even if legal restrictions do not technically apply. And a set of more specifically legal issues does arise with respect to free third-party software, such as with terms of service agreements and logos.

The Obama administration should encourage the use of Web 2.0 technologies, and lead the way on WhiteHouse.gov, but it must do so in a way that is compliant with federal law, and also in the spirit of the law. In other words, the White House New Media team should continue to work with the General Services Administration to negotiate agreements that encourage Web 2.0 companies to ensure greater protection and accessibility for users, even if it is not legally necessary.

Each of the six hurdles to implementation have their own intricacies, and the following report analyzes each and provides recommendations for how the Obama administration can move forward both quickly and legally.

1. Privacy and Freedom of Information Act compliance

Web 2.0 technologies raise at least three distinct privacy issues: whether third-party applications can use persistent cookies even though they are prohibited on federal websites that ban its use; whether users should receive the same level of privacy as on federal websites; and whether Web 2.0 activities would be subject to the Freedom of Information Act.

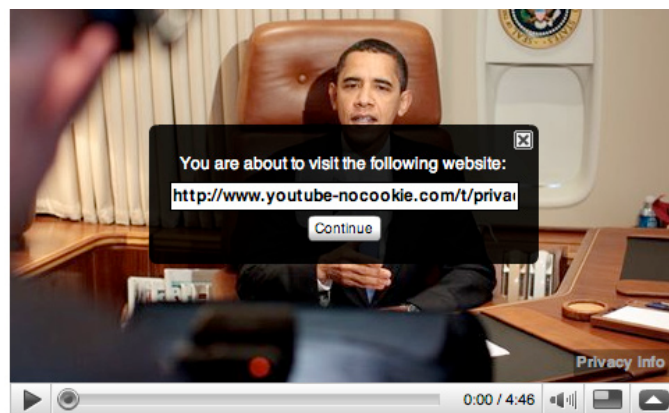
Persistent cookies

The Office of Management and Budget has issued government-wide guidance on the use of persistent cookies—technology that identifies the same computer in multiple sessions of browsing—on federal websites. It released two guidelines in 2000: Memorandum 00-13, “Privacy Policies and Data Collection on Federal Web Sites,”¹ and a letter from OMB Office of Information and Regulatory Affairs Director John Spotila.² The memorandum states that:

“... The presumption should be that ‘cookies’ will not be used on Federal websites. Under this new Federal policy, ‘cookies’ should not be used at Federal websites, or by contractors when operating websites on behalf of agencies unless, in addition to clear and conspicuous notice, the following conditions are met: a compelling need to gather the data on the site; appropriate and publicly disclosed privacy safeguards for handling of information derived from ‘cookies’; and personal approval by the head of the agency.”

WhiteHouse.gov and federal agencies wishing to use persistent cookies can negotiate with Web 2.0 companies to gain access to versions of applications that do not include cookies. YouTube, for example, provided WhiteHouse.gov with a cookie-free version of its video player, which the site has used on its blog and for the president’s weekly video address. The OMB guidance also permits agency heads to grant waivers for the cookies restrictions.

There are sharply different views about how to proceed on persistent cookies. The Federal Web Managers Council favors immediate repeal of the



download .mp3 or HD .mp4 (51.5 Mb) | also available here | read prepared remarks

2000 OMB guidance on cookies, saying it “greatly limits our ability to serve customers’ needs because our sites can’t remember preferences or settings. It also means we can’t take advantage of sophisticated web services and analytic tools that rely on persistent cookies.”³

Yet privacy advocates will likely object if there is an immediate repeal. The Center for Democracy and Technology, for instance, has written a paper urging retention of the policy.⁴ It would therefore be better from a privacy policy perspective for the Obama administration to modify the cookie policy as part of an overall package that includes policies that show it plans to offer strong policy protections. The administration should also coordinate with independent agencies including the Federal Trade Commission and the Federal Communications Commission, which are engaged in policy issues regarding how tracking technologies should be used for advertising and other online activities.

The Obama administration could also seek additional information from the Federal Web Managers Council and the White House New Media department. These groups can help pinpoint how the OMB guidance affects the use of Web 2.0 applications by government sites and offer insight into how difficult or effective the process of getting persistent cookie approval from agency heads has been in the past.

Some uses of persistent cookies are similar for federal and private websites, such as using cookies to collect analytics about how individuals navigate the website in order to make the site more useful. Other uses of cookies, however, are different in the federal government. For instance, federal websites do not have advertising and therefore do not need to use cookies to document to advertisers the numbers of unique visitors to each page. Federal web managers can create a more informed basis for assessing possible changes to the 2000 OMB guidance to the extent that they show improved government function by using cookies.

The Center for Democracy and Technology, or CDT, and the Electronic Frontier Foundation have begun a useful project to explore specific privacy issues that arise in federal Web 2.0 applications. CDT recently released its first report concerning web analytics—the tools that webmasters can use to measure site traffic in order to improve performance.⁵ This sort of detailed analysis of different use scenarios and their effects on privacy provides the foundation to update the 2000 guidance.

User data on third-party websites

The Privacy Act of 1974 dictates that, “No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains.” This applies to all federal websites, but it does not apply to activities on non-federal websites.⁶ This means that, as the Federal Web Managers Council has stated, “There is no guarantee that social media sites will protect people’s privacy to the same degree as federal agencies.”⁷

The federal government is responsible, however, for making sure that users are notified whenever they are leaving an official federal website and are thus subject to the policies of the Web 2.0 provider. When WhiteHouse.gov recently launched its Facebook, MySpace, and Twitter pages, users saw a “splash page” that announced, “You are exiting the White House server” and gave the URL of the Web 2.0 application that would next appear.

This sort of prominent notice is entirely appropriate. It alerts the users that they are leaving a government website and identifies the company providing the Web 2.0 service, so that the user can choose to view that service’s privacy policy. Overtime, however, federal agencies should likely explore a more proactive approach to ensuring privacy on Web 2.0 pages to which they link. Web 2.0 companies want the prestige, brand recognition, and click-throughs that come from being listed on WhiteHouse.gov or other federal sites. Federal agencies should therefore compare shopping on privacy and negotiating to bring Web 2.0 providers up to higher privacy standards.

One specific concern has been raised about federal websites’ use of social networking sites. If an individual “become[s] friends with a company or an agency, its employees can see the information you share with your other friends.”⁸ If a Web 2.0 site has this sort of privacy-invasive feature, then the federal agency can simply announce in its own privacy policy that it will not look at that sort of information.

The Freedom of Information Act

It is possible that lists of names and/or email addresses of those participating in federal Web 2.0 activities may be made public in response to Freedom of Information Act requests. FOIA provides a privacy exception for “personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.”⁹ But it is not clear how the FOIA exception would apply to e-mail lists or other information from individual participants in Web 2.0 activities.

It will be important for the Obama administration to encourage confidence in federal Web 2.0 activities so that users aren’t dissuaded out of concern for their privacy. The administration should therefore provide government-wide guidance indicating that these categories of information should be protected under the § 552(b) (6) privacy exception. This guidance would likely come from the Department of Justice, perhaps accompanied by statements from the Office of Management and Budget.

Recommendations

Persistent cookies

- WhiteHouse.gov has already negotiated with YouTube to use a version of the embeddable video player that does not include persistent cookies. WhiteHouse.gov and GSA can lead the way in negotiating similar solutions with other Web 2.0 companies so that the federal government can use these technologies without violating OMB policy.
- The Obama administration should begin to work on a more long-term solution on persistent cookies that addresses the complexity of the issue, the conflicting views of privacy and new media advocates, and the public policy debates about online advertising. The solution would likely involve making changes to, but not revoking, the OMB memorandum that prevents the use of persistent cookies on federal websites without a waiver from the agency head. The administration should seek public comments as part of the revision process due to stakeholder interest in this issue.

Privacy on third-party websites

- WhiteHouse.gov and all other federal websites should provide a disclaimer making it clear to users when they leave an official federal website. This will convey to users that they will be subject to the outside website's policies and not the government's.
- Privacy should be one of the factors that the federal government considers when it selects third-party Web 2.0 services, which can help improve private-sector privacy practices over time. Federal agencies may be able to negotiate improvements in the privacy policies of Web 2.0 services that want to serve the federal government.
- If a social networking or other Web 2.0 application allows more access to personal information than is appropriate, the agency can announce in its own privacy policy that it will not access that information.

Freedom of Information Act

- The Obama administration should offer government-wide guidance that e-mail addresses and similar information collected in the course of Web 2.0 activities, and not publicly posted, should be protected under the FOIA's § 552(b)(6) privacy exception. This will help ensure user confidence in the privacy of personal opinions and information.

2. Access for people with disabilities

Section 508 of the Rehabilitation Act of 1973 requires federal websites to provide individuals with disabilities access to and use of website information and data that is comparable to that provided to the general public.¹⁰ Each agency must ensure that such electronic information technology is accessible to individuals with disabilities unless an undue burden would be imposed on the agency. When compliance imposes an undue burden, Section 508 requires agencies to at least provide the information by an alternative means that allows disabled individuals access to it. Alternate methods may include, but are not limited to, voice, fax, relay service, TTY, Internet posting, captioning, text-to-speech synthesis, and audio description.

WhiteHouse.gov under President Obama has taken substantial steps to become accessible. In contrast to the campaign, which posted many videos that were not closed-captioned, WhiteHouse.gov now includes captioning on videos and also provides a text transcript for audio clips.¹¹ To assist visually-impaired people, images on WhiteHouse.gov contain “alt tags,” which aid users who listen to the content of the site by using a screen reader, rather than reading the site. The White House has also asked users with disabilities to review the site and solicits comments on how to make the site more accessible.

All federal agencies are required to comply with Section 508 when they “develop, procure, maintain, or use” electronic or information technology. Section 508 sets a high standard for access for compelling reasons—government communications should be available to all Americans, including those who have visual, auditory, or other disabilities. Section 508 thus expects more of federal agencies— such as the use of alt tags or captioning for videos— than is general practice for private websites. Federal webmasters, working with the U.S. Access Board, have developed expertise in efficient ways to assure accessibility.

The rise of Web 2.0 technologies presents new issues on how Section 508 will apply. The question is when the “use” of Web 2.0 software is substantial enough to trigger Section 508 requirements. Some uses clearly are not substantial enough. For instance, Section 508 should not require federal employees to only use Section 508-compliant search engines, news sites, or videos.

The question becomes tougher when a federal agency makes more substantial “use” of offsite resources. For instance, a federal agency site might hyperlink to content on another site. Should hyperlinks be allowed only to Section 508-compliant URLs? That policy, in

my view, would be too strict—it would prevent the agency from linking to a potentially wide range of useful content, and it is often difficult for a federal employee even to determine whether another website complies with disability rules.

An even harder question is what an agency’s Section 508 approach should be when it wishes to have an ongoing presence on Web 2.0 sites, such as an agency “channel” on YouTube or an agency page on MySpace or Facebook. In favor of requiring Section 508 compliance, one could argue that an agency YouTube channel triggers disability requirements because it counts as agency “use” of electronic or information technology. On the other hand, the channel exists apart from the agency website and resides on private-sector computers, and the agency is required to alert users when they leave the official agency site.

The accompanying paper on federal procurement of Web 2.0 software proposes a middle path on this issue. That paper describes a “conditional use” approach that would allow federal agencies to sign terms of use to create an ongoing presence on Web 2.0 sites, but the government should negotiate for conditions, in government-wide agreements, that push private websites toward Section 508 compliance. The government can make greater use of private-sector software that offers good accessibility, hence making both government and private-sector sites more accessible for more Americans.

Key 508 compliance standards

Section 508 compliance lays out requirements for various formats of web-based information and applications. The following list includes some of the key regulations and examples of how such content can be made compliant:¹²

1. Every non-text element needs a text equivalent. For example, by including “alt” tags on images and transcripts for videos.
2. Equivalent alternatives must be provided synchronously for all multimedia presentations, for example, closed captioning for videos.
3. All web pages must be designed so that all information conveyed with color is also available without color, making it accessible for the colorblind. This can be accomplished, for example, by ensuring there are markup descriptions or that images can be understood through context.
4. All documents must be organized so they are readable without requiring an associated style sheet.
5. Image maps, or visual objects that include links, must also provide redundant text links.
6. All data tables must include row and column headers, and tables with two or more levels of headers must include markup that associates data and header cells.
7. Any information that utilizes scripting languages, plug-ins, or applets must also be provided with functional text that can be read by assistive technology.
8. Electronic forms designed to be completed online must allow people using assistive technology to access the information, and complete and submit the form.
9. Websites must alert users whenever there is a timed response limit and provide them with sufficient time to indicate that more time is required.

Recommendations

- The Obama administration must make sure that all materials on WhiteHouse.gov are Section 508 compliant. If there are applications for which Section 508 compliance would pose an undue burden, it should at least provide the information in a format that is available to individuals with disabilities.
- When linking to outside sites that may not be Section 508 compliant, executive branch websites should display a splash message to users that indicates that they are leaving a federal website.
- WhiteHouse.gov and agency websites should encourage social media sites that they use to make their sites Section 508 compliant. The executive branch should use compliance as a criterion for deciding whether to link to a site or sign terms of use for Web 2.0 software
- The Obama administration should have the Chief Technology Officer or OMB issue guidance to agencies requiring that they post their materials in accessible formats on their own websites, rather than having non-governmental sites be the sole location where content is posted. This will ensure that people with disabilities have an accessible version of the content, and that the official version of content is located on a government website. The CTO and OMB can and should also work with the General Services Administration to develop a procurement process for purchasing tools that may assist with Section 508 compliance, such as captioning software to make videos and webcasts available to people with disabilities.

3. Commercial endorsement and advertising

There are longstanding policies against using advertising on federal websites or having sites endorse specific software or other products. Current General Services Administration guidelines prohibit .gov websites from commercially endorsing any product, commodity, or service.¹³ GSA guidelines also prohibit non-government advertising on .gov sites.¹⁴ These rules, and the policies underlying them, raise questions about whether choosing specific Web 2.0 applications over others constitutes a commercial endorsement and whether advertising on the third-party sites would prohibit the government from using them.

From the perspective of a press office, there can be significant advantages if views are concentrated in one popular application. It can create a “virtuous circle” for popularity: if a video becomes popular, for example, it might become a “most viewed” item on the Web 2.0 site’s “news and politics” category, thus garnering additional views. Furthermore, once on the “most viewed” page for “news and politics,” it might climb to the top of that category and get on the front page for the entire video site, getting even more views. Concentrating viewers in a leading Web 2.0 application is similar to putting a spokesman on a popular television show or granting an interview to a major newspaper—these are techniques for increasing viewership and getting the message out more effectively.

The Obama new media team was widely admired during the campaign for its ability to use YouTube and other Web 2.0 software to get the message out and generally assist the campaign. In shifting to the government, however, the issue of commercial endorsement became more prominent, especially in connection with President Obama’s weekly video addresses. The weekly addresses were initially posted only on YouTube during the transition, and the YouTube logo was visible while viewing the video. This approach achieved a high number of viewers, but press stories understandably asked why the president should endorse only one video channel.¹⁵

The format for the weekly radio address has since expanded well beyond the original YouTube-only stream. The May 9 weekly address, for instance, provided streaming from either YouTube or Vimeo, and company logos are not visible to the user on either player. The video was also downloadable in either the mp3 or mp4 formats. The “share/bookmark” feature linked to 10 different destinations, beginning in alphabetical order with Delicious, Digg, and Facebook.

From the point of view of commercial endorsement, this range of formats is a clear improvement over the YouTube-only approach inherited from the campaign. The government should avoid publicly endorsing one product or service over its competitors. As discussed in the accompanying paper on procurement, the government goes through a formal process to award “concessions” in some settings, such as restaurants that pay the government to operate in a national park. Looking forward, it may make sense to use this formal concessions process for high-value activities such as the White House weekly address. For most agency activities, however, it is likely not worth going through a formal concessions process, and federal agencies should steer clear of endorsing specific products or services.

The advertising and endorsement restriction generally should not be a major barrier to Web 2.0 activity on federal websites. Sites are permitted to link to private websites that contain advertising as long as a splash page informs users that they are leaving the website. Current guidelines require that, “When a link on a Gov Internet domain makes the user leave a Gov Internet website, a notification or screen (for example, a splash message) should alert users that they are leaving the official Gov Internet page.”¹⁶ This is widely and consistently used on WhiteHouse.gov and all other federal websites.

Nevertheless, The White House has had success with getting Web 2.0 sites that contain advertising to remove it on pages where the administration has a presence. The White House’s Facebook and MySpace social network pages, for example, contain none of the usual advertising that is included in the sidebar and header of other users’ profiles.

Recommendations

- WhiteHouse.gov should continue to provide embeddable videos in an open format that allows users to download the videos, cut and paste them, and post them on other sites. When possible, WhiteHouse.gov may also embed or provide links to other free services that host such videos.
- The White House should continue to negotiate terms of service with free service providers, including terms that would allow removal of their logos from material that appears on WhiteHouse.gov.
- The Obama administration should consider revising the .gov guidelines by clarifying that the mere use of a free service does not constitute commercial endorsement of that service.
- Federal websites are not legally responsible for advertising that appears on third-party websites, but agencies should consider whether the outside sites contain inappropriate advertising or content when deciding which services to use.

4. Terms of service

Many websites require account owners to agree to terms of service such as indemnification provisions that make clear who is legally liable in certain situations. They also often assert that a particular state's laws will be used to adjudicate disputes. These commonly used terms of service pose an obstacle to federal use of Web 2.0 software. The Anti-Deficiency Act states that federal employees and agencies are not permitted to accept indemnification agreements or agree to pay a site's legal costs for disputes involving an account owner.¹⁷ The Supremacy Clause of the U.S. Constitution means that federal law—and not state laws—applies to the federal government's activities.

The federal government's basic approach to this problem should be to negotiate terms of use that comply with federal requirements. There were no WhiteHouse.gov or government-wide terms of service for Web 2.0 technologies before 2009, but that has changed considerably in the Obama administration's opening months. By the end of April, 2009, the General Services Administration had negotiated standards terms of service for use government-wide for Facebook, MySpace, Flickr, YouTube, Vimeo, Blist, Slideshare, AddThis, and blip.tv.¹⁸

The high visibility and traffic on WhiteHouse.gov was almost certainly one motivation for these companies to adopt terms of service that complied with federal requirements. In addition, the ability to negotiate one agreement government-wide reduced negotiation and other costs both for the companies and for agencies that would have found it more difficult to negotiate on their own for required federal terms of service.

If an important Web 2.0 service refuses to negotiate, the administration might consider alternative approaches. For instance, the government can declare certain terms of service provisions to be null and void by announcing that the federal government cannot lawfully enter into agreements for Web 2.0 services that require indemnification and the application of state law under the Anti-Deficiency Act and the Supremacy Clause of the Constitution. This sort of announcement could be useful in negotiations with Web 2.0 providers, underscoring that federal agencies lack the authority to be bound by such provisions. This approach is politically blunt, however, and further legal consultation with federal contracting experts may clarify the extent to which this approach is feasible.

Any of these options can and should be combined with specific authorization for federal agencies to continue to negotiate on a case-by-case basis the terms of service of Web 2.0 technologies. Agencies should not need to wait for GSA to negotiate a government-wide agreement before experimenting and using Web 2.0 technologies.

One troublesome item to date is that GSA has not made the government-wide terms of service public.¹⁹ One might understand why some Web 2.0 providers would prefer to keep these terms of service confidential—they may have agreed to terms for the federal government that they do not wish to make available to all users. And the agencies may have an incentive to agree to confidentiality if that is a condition for getting better terms for the federal agencies. With that said, the default policy should ensure that individuals know the privacy, security, and other rules that apply when they interact with a federal agency. Public disclosure is at least appropriate for the terms of service that apply to individual users.

Recommendations

- The General Services Administration, in consultation with those running WhiteHouse.gov, should identify any problematic terms of service for Web 2.0 applications and move forward on negotiating these specific terms of service.
- The administration should conduct further research on federal contracting law to identify the extent to which it can declare terms of service “null and void.”
- GSA and the Federal Web Managers Council should continue their good start at negotiating government-wide terms of service with Web 2.0 providers.
- The default should be to make public terms of service, especially for privacy, security, and other topics that affect individual users.

5. Paperwork Reduction Act compliance

The Paperwork Reduction Act requires agencies to submit formal requests to the Office of Management and Budget before collecting information from the public.²⁰ Web 2.0 activities on WhiteHouse.gov and agency sites will often solicit comments and other feedback from users, which raises questions about whether the Act would include such interactive information technology.

The Paperwork Reduction Act specifically requires federal agencies to submit a formal request to OMB,²¹ when “obtaining, causing to be obtained, soliciting, or requiring the disclosure to an agency, third parties or the public of information by or for an agency by means of identical questions posed to, or identical reporting, recordkeeping, or disclosure requirements imposed on, ten or more persons, whether such collection of information is mandatory, voluntary, or required to obtain or retain a benefit.”²²

In other words, a federal agency has to get permission to collect any information that it wants to gather from 10 or more people. The type of collection that the PRA covers is very broad, including everything from questionnaires and surveys to personal data, disclosure requirements, and general agreements.²³

Fortunately, much of the activity that would occur in a Web 2.0 forum is specifically exempted from the Act. The statute does not cover “facts or opinions submitted in response to general solicitations of comments from the public, published in the Federal Register or other publications, regardless of the form or format.”²⁴ The PRA would therefore not pertain to comments on an agency or White House website—as long as users aren’t required to submit any personal information beyond self-identification in order to submit their thoughts and are not surveyed for more specific information.

One example that the White House has already implemented is on recovery.gov. The website presently collects user stories in the “Share your Recovery Story” section of the website. The link to the section states:

Tell us how the Recovery Act is affecting you. What's working? What isn't? We want to hear from you.

Users are then taken to a page where the only required information is the user's name and email address. Because "no person is required to supply specific information pertaining to the commenter, other than that necessary for self-identification, as a condition of . . . full consideration of the comment," this type of solicitation does not trigger the PRA requirements.

If the White House or other agencies would like to survey users and collect information beyond general comments in the future, or require users to provide more than self-identifying information, they will run up against the Paperwork Reduction Act. The administration should likely update these regulations to allow collection of such data in Web 2.0 forums. The administration may also consider reviewing Presidential Records Act requirements and other archiving rules to ensure that records are kept for government activity without imposing unnecessary burdens in record-keeping for private-sector activity on private websites.

The screenshot shows the RECOVERY.GOV website. The header includes the logo and navigation links: HOME, ABOUT, INVESTMENTS, OPPORTUNITIES, IMPACT, NEWS, FAQ, CONTACT US. A 'Sign up for updates' link is also present. Below the header, there is a breadcrumb trail: Home > Share your Recovery Story. The main heading is 'SHARE YOUR STORY'. The text explains that the economic crisis has affected everyone and that the American Recovery and Reinvestment Act is designed to provide relief. It asks users how they are affected by the crisis, whether as an employer, student, or job-seeker. It mentions that in a few months, the site will allow users to peruse extensive data to measure progress. It encourages users to share their story now. Below the text, there is a form with the following fields: First Name (*), Last Name (*), E-mail (*), Address, City, State (dropdown menu with 'Select a State' and a plus sign), ZIP Code (two input boxes), and Phone. There is also a large text area for 'Share your experience. *' and a 'SUBMIT' button at the bottom.

Recommendations

- The Paperwork Reduction Act does not impose restrictions when agencies only gather a user's name and e-mail address, but more detailed inquiries to the public require OMB permission.
- OMB may find it appropriate to draft new regulations to facilitate detailed user surveys about federal use of Web 2.0 technologies. OMB should also study whether other data collection occurs in the use of Web 2.0 technologies that should not trigger burdens under the Paperwork Reduction Act.

6. Computer security and use of Web 2.0 by federal agency employees

Many federal agencies have blocked their employees from accessing social media websites and chat functions on their government computers. There is no legal restriction or policy guidance that requires blocking employee access to such websites and functions, but agencies cite concern such as security, productivity, and bandwidth availability.

The increasing deployment and usefulness of Web 2.0 means that agencies should only block employee access upon careful analysis. For instance, as the White House and other agencies increasingly make use of Web 2.0 applications, federal employees may be cut off from accessing official government communications and contributions from the public that exist on such websites. Blockage is especially counterproductive for employees who have new media and communications functions for the agency—such employees' jobs could be restricted substantially if they are blocked from using the most effective Web 2.0 communications tools.

Some Web 2.0 software may present computer security risks. An even bigger risk may come from applications that plug into Web 2.0 software platforms. For instance, a federal agency may be able to configure Facebook in ways that meet agency privacy and security criteria, but would find it time consuming to do a similar check on every one of the thousands of Facebook applications that are now available.

Federal agencies should develop more thorough procedures going forward to enable Web 2.0 technologies where appropriate while maintaining security. GSA, the Federal Webmasters Council, and individual agencies may be able to develop white lists of secure applications and black lists of insecure applications. Federal agencies should share configurations for common Web 2.0 applications that are more secure, and should encourage Web 2.0 providers to supply information about secure settings.

Recommendations

- Federal agencies should not block use of web 2.0 applications except for good reason, such as significant security risks. The Office of Management and Budget should consider guidance to agencies in favor of providing federal employee access to social media sites. The presumption should be especially strong for employees engaged in new media and public communications functions. Access could be blocked only when a senior agency official justifies blocking certain employees or certain sites.
- GSA, the Federal Webmasters Council, and federal agencies should share information about the security of Web 2.0 applications, including information about settings that enable employee access while minimizing security risks.

Endnotes

- 1 Office of Management and Budget, "Memorandum For The Heads Of Executive Departments And Agencies," June 22, 2000, available at <http://www.whitehouse.gov/omb/memoranda/m00-13.html>.
- 2 Office of Management and Budget, "Cookies Letter," September 5, 2000, available at http://www.whitehouse.gov/omb/inforeg/text/cookies_letter90500.html.
- 3 Bev Godwin and others, "Social Media and the Federal Government: Perceived and Real Barriers and Potential Solutions," December 23, 2008, available at http://www.usa.gov/webcontent/documents/SocialMediaFed%20Govt_BarriersPotentialSolutions.pdf.
- 4 Ari Schwartz, "A New Cookie Policy for eGov 2.0 – Part I," (Washington: Center for Democracy and Technology, January 2009), available at <http://blog.cdt.org/2009/01/08/a-new-cookie-policy-for-egov-20-%E2%80%93part-i/>.
- 5 Center for Democracy and Technology, "Open Recommendations for the Use of Web Measurement Tools on Federal Government Web Sites," May 2009, available at http://www.cdt.org/privacy/20090512_analytics.pdf.
- 6 The Privacy Act does apply to subcontractors who operate a system of records on behalf of a federal agency. Where an individual chooses to leave a federal website and begin surfing at a private Web 2.0 site, however, the Privacy Act does not apply.
- 7 Bev Godwin and others, "Social Media and the Federal Government: Perceived and Real Barriers and Potential Solutions," December 23, 2008, available at http://www.usa.gov/webcontent/documents/SocialMediaFed%20Govt_BarriersPotentialSolutions.pdf.
- 8 Saul Hansell, "Should the White House Be a Place for Friends?" available at <http://bits.blogs.nytimes.com/2009/05/04/should-the-white-house-be-a-place-for-friends/?apage=1>
- 9 Freedom of Information Act of 1974, 5 U.S.C. § 552(b)(6).
- 10 Rehabilitation Act of 1973, 29 U.S.C. § 794d.
- 11 The White House, "Accessibility," available at <http://www.whitehouse.gov/accessibility/>
- 12 36 CFR § 1194.22.
- 13 The current .gov guidelines state: "A Gov Internet domain may not be used to ... imply in any manner that the government endorses or favors any specific commercial product, commodity, or service." 41 CFR § 102-173.95, available at http://www.dotgov.gov/program_guidelines.aspx.
- 14 Ibid.
- 15 Dan Farber, "Obama Appoints YouTube (Google) as Secretary of Video," November 16, 2008, available at <http://news.cnet.com/obama-appoints-youtube-google-as-secretary-of-video/>.
- 16 41 CFR § 102-173.95, available at http://www.dotgov.gov/program_guidelines.aspx.
- 17 Anti-Deficiency Act, 13 U.S.C. § 1341.
- 18 U.S. General Services Administration, "GSA Takes Another Big Step Forward," available at http://www.gsa.gov/Portal/gsa/ep/contentView.do?contentType=GSA_BASIC&contentId=27992&noc=T.
- 19 Democratic Media, "Federal Gov't (GSA) Refuses to Make Public Agreements with Facebook, MySpace, etc. Is data from individuals seeking gov't information going to these sites?" April 30, 2009, available at <http://www.democraticmedia.org/jcblog/?p=801>
- 20 Paperwork Reduction Act of 1996 44 U.S.C. § 3501 et. seq.
- 21 This reporting requirement applies widely to "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency," although it excludes "the General Accounting Office, the Federal Election Commission, the governments of the District of Columbia and of the territories and possessions of the United States, and their various subdivisions, and Government-owned contractor-operated facilities."
- 22 5 CFR § 1320.3(c).
- 23 "A collection of information may be in any form or format, including the use of report forms; application forms; schedules; questionnaires; surveys; reporting or recordkeeping requirements; contracts; agreements; policy statements; plans; rules or regulations; planning requirements; circulars; directives; instructions; bulletins; requests for proposal or other procurement requirements; interview guides; oral communications; posting, notification, labeling, or similar disclosure requirements; telegraphic or telephonic requests; automated, electronic, mechanical, or other technological collection techniques; standard questionnaires used to monitor compliance with agency requirements; or any other techniques or technological methods used to monitor compliance with agency requirements. A collection of information may implicitly or explicitly include related collection of information requirements."
- 24 5 CFR § 1320.3(h)(4).

The Center for American Progress is a nonpartisan research and educational institute dedicated to promoting a strong, just and free America that ensures opportunity for all. We believe that Americans are bound together by a common commitment to these values and we aspire to ensure that our national policies reflect these values. We work to find progressive and pragmatic solutions to significant domestic and international problems and develop policy proposals that foster a government that is “of the people, by the people, and for the people.”

Center for American Progress

