THE INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

Federal Government Policy on the Use of Persistent Internet Cookies: Time for Change or More of the Same?

BY DANIEL CASTRO | MAY 2009

Federal government agencies need flexibility to create new online content and applications without unnecessary restrictions on the use of particular technologies.

In the digital world, a decade is a long time. A decade ago many web sites—both government and commercial—started to use "cookies," small data files stored on a user's computer by a web browser to improve the web user's experience. However, in part from a lack of understanding of this new technology, and because of an outcry by some privacy advocates against the use of cookies, in 1999 the Clinton administration implemented strict limitations on the use of persistent cookies on federal government agency websites. Notwithstanding the fact that cookies are in widespread use on commercial and state and local government websites, this federal policy has seen little change in the past ten years.

The result of these limitations is that federal web pages are less useable and citizen-friendly than they otherwise could be. Government agencies need flexibility to create new online content and applications without unnecessary restrictions on the use of particular technologies. **The Obama administration should adopt new policies for government websites that balance privacy against other equally important goals such as usability, accessibility and transparency.** This should include updating website privacy policies to use standard language across government agencies and to specify the activities permitted and restricted by the government websites. In addition, the Office of Management and Budget (OMB) should publish regularly updated guidelines outlining permitted uses of persistent cookies and guidance on best practices, such as the maximum lifespan of persistent cookies. The goal should be to create policies that facilitate, rather than hinder, the adoption of new web technologies, including those that use cookies.

This report 1) provides a background on cookies and their use; 2) reviews the history of the government decision to strictly limit persistent cookies on federal government agency websites; 3) compares the use of persistent cookies on mainstream commercial websites and government websites; 4) analyzes the implications of the current federal government policies on the use of persistent cookies and discusses how changing this policy might enable better e-government services; and 5) proposes a new framework for the use of cookies on federal government websites.

BACKGROUND

Government has an important role to play in protecting the privacy of its citizens in both the online and offline world. As we enter an increasingly digital world, many privacy advocates have raised concerns about the potential loss of privacy as organizations use IT to collect large amounts of data. In particular, advocates have worried that the ease with which information can be collected online represents a serious threat to the privacy of individuals.

One of the first major online privacy risks raised by advocates was the use of HTTP cookies—small data files stored on a user's computer by a web browser. When a user visits a website, the website can request that the user's web browser store certain data in a cookie. By default, most web browsers allow this activity. A cookie may be used to store temporary data, such as the contents of a shopping cart for e-commerce, or to remember a user on subsequent visits to the website, such as for customizing a website. Each cookie is accessible only by the Internet domain that created the data.[1]

For many privacy advocates the risk from cookies is as follows: under some circumstances, cookies can be used to help website operators track website usage over time and build a profile of user activity. In addition, if the website collects personally identifiable information, the website operator could potentially link some browsing activity to individual identities. This could potentially lead to the intentional or accidental disclosure of an individual's web browsing history—a clear violation of a user's expected level of privacy. Privacy advocates see the collection and misuse of such data to be the primary threat of cookies.

However, cookies also offer many benefits. Website developers use cookies to develop robust online applications that create a better user experience. Perhaps the most common use of cookies is to facilitate online commerce. Online shopping cart applications routinely use cookies to maintain the list of which items a shopper wants to purchase. In addition, if the user accidentally closes the web browser or the browser crashes, the user can often return to the website without having to reload items back into the shopping cart. Cookies facilitate these functions transparently to the user. Cookies also enable users to customize websites. For example, users can personalize settings such as preferred language or region so the website will recognize their preferences on subsequent visits. Weather.com uses cookies to remember a returning user's zip code and automatically displays the weather report for that user's geographic area. For websites requiring a login, cookies can be used to authenticate users so that the user does not have to always enter a username and password to access a website. Website operators also use cookies to learn how to best engage with their audience and measure the success of online content and online advertising. Cookies help website developers produce more advanced website analytics to better understand how users interact with their website. For example, cookies allow website developers to learn how many of their visitors are new or returning users.

While cookies can be used to enable targeted advertising to deliver more relevant website ads, users can also employ cookies to opt-out of targeted online advertising.

Cookies can be classified based on the source of the cookie and the lifespan of the cookie. When classified by the source, cookies come in two flavors: first-party cookies and third-party cookies. First-party cookies refer to cookies created by the domain of the website that the user entered in the web browser. Third-party cookies are those created by affiliated domains, such as advertising networks used by the primary website visited by the user. For example, a user that visits CNN.com not only will receive cookies for CNN.com, but also for other domains used by online advertisers employed by CNN, such as doubleclick.net, revsci.net, and questionmarket.com.[2] Advertisers can use third-party cookies to track user preferences across multiple websites for targeted advertising. All major web browsers include the option to block third-party cookies.

When classified by lifespan, there are two types of cookies: session cookies and persistent cookies. Session cookies, as the name implies, last only as long as the user is on a particular website. Session cookies enable websites to remember data about users as they navigate from page to page on the same website.[3] For example, session cookies enable technologies like online shopping carts. Persistent cookies last beyond the initial web browsing session. The cookies can be set to expire at a certain time or last indefinitely.[4] These types of cookies are useful so that a website can recognize a returning user. For example, a website can use a persistent cookie to recognize a user on return visits, thus saving the user from having to log in at every visit.

While, as described above, cookies can be used to enable targeted advertising to deliver more relevant website ads, users can also employ cookies to opt-out of targeted online advertising. As explained by DoubleClick, a major online third-party advertiser, Internet users can replace DoubleClick's DART cookie with an opt-out cookie so that "ads delivered to your browser on behalf of clients using DoubleClick's ad-serving technology will be targeted based only on the non-personally identifiable information that is automatically transmitted in the Internet environment when an ad request is received by our ad servers, and your DART cookie will not be uniquely identified."[5] Most third-party online advertisers participating in the Network Advertising Initiative have also made a similar opt-out tool available online for users to more easily avoid targeted online advertising.[6] The point of this example is not to argue for or against behavioral advertising, but merely to show that cookies can be used to both enable and disable targeted advertising.

FEDERAL GOVERNMENT POLICY ON COOKIES

The Office of Management and Budget (OMB) in the Executive Office of the President released the first major federal government directive on website privacy in June 1999. Jacob Lew, Director of OMB, issued a memo directing all departments and agencies to "post clear privacy policies" on all government websites.[7] The memo included additional guidance and model language for federal website privacy policies. The only model language directly dealing with cookies came from the Social Security Administration's (SSA) privacy policy. The SSA's privacy policy restricted all use of cookies, both session cookies and persistent cookies.[8]

The issue received widespread media attention in June 2000 when the White House announced that the Office of National Drug Control Policy (ONDCP), in partnership with DoubleClick, had used cookies as part of an online anti-drug advertising campaign. The cookies helped measure the efficacy of the online campaign by tracking what ads were clicked, the number of users that clicked the ads, and what pages these users subsequently viewed on the ONDCP website.[9] Without these metrics, ONDCP would not have been able to measure the effectiveness of its online campaign. Some privacy advocates strongly objected to the campaign and, as a result of their public criticism, the incident became known as "Cookiegate" in the press.[10] For example, Marc Rotenberg, the Executive Director of the Electronic Privacy Information Center, framed the incident as a case of intrusive government tracking of its citizens' behavior. Even though neither ONDCP nor DoubleClick collected personally-identifiable information, Rotenberg wrote, "Monitoring citizens' use of government Web sites raises profound privacy and constitutional concerns."[11]

Federal regulations for government websites should emphasize privacy; however, privacy should not be emphasized at the expense of other laudable goals for e-government such as usability, transparency and accessibility.

This was part and parcel of a general level of concern about cookies at the time; a concern that over time has been shown to be overblown. Initially, some policymakers, in the White House and elsewhere, reacted strongly against the use of cookies, mostly because of a lack of understanding of the technology. In 2000 at a forum on Internet privacy, upon learning that his personal computers in his home and office likely contained cookies, former Senator Bill Frist asked "How do I turn it off?"[12] In 2001, the European Parliament even went so far as to consider a proposal that would have effectively prohibited the use of cookies on both government and commercial websites. Fortunately, the proposal did not pass after the Internet Advertising Bureau UK initiated a "Save our Cookies" campaign to educate lawmakers about the benefits of cookies.[13]

In response to public pressure, the Clinton White House immediately directed ONCDP to terminate the program. OMB almost immediately released a memo issuing new guidelines restricting the use of cookies on federal government websites. The new June 2000 OMB policy was as follows:

> Because of the unique laws and traditions about government access to citizens' personal information, the presumption should be that "cookies" will not be used at Federal web sites. Under this new Federal policy, "cookies" should not be used at Federal web sites, or by contractors when operating web sites 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.[14]

The State of Idaho uses persistent cookies on its website so that a resident applying for a license online can resume an existing application without losing any data even if the session is interrupted

In other words, the default policy of all government websites was to not use cookies. OMB revisited this policy a few months later in response to a letter from Roger Baker, the Chief Information Officer (CIO) at the U.S. Department of Commerce and Chairman of the CIO Council subcommittee on Privacy.[15] In a letter dated September 5, 2000 OMB clarified that the earlier guidance applied to session cookies but did not apply to persistent cookies. As OMB stated in the letter:

> [Agency web sites] may retain the information only during the session or for the purpose of completing a particular online transaction, without any capacity to track users over time and across different web sites. When used only for a single session or transaction, such information can assist web users in their electronic interactions with government, without threatening their privacy. One example of such an approach that supports electronic government would be the use of a shopping cart to purchase a number of items online from the U.S. Mint. Another example would be the current technology that assists users in filling out applications that require accessing multiple web pages on the Department of Education's Direct Consolidation Loan site. We do not regard such activities as falling within the scope of [the June 2000 memo].[16]

In October 2000, the Government Accountability Office (GAO) issued a report reviewing the use of persistent cookies on federal government websites. In a survey of 65 websites, GAO reported that eight websites used first-party persistent cookies (four without an appropriate disclosure in the website privacy policy and four with the appropriate disclosure) and three websites used third-party persistent cookies without an appropriate disclosure.[17] GAO revisited the issue in January 2001 and found that of the 65 websites reviewed, eight were still using persistent cookies. Of those eight websites, four did not give appropriate notice in their privacy policy. Of the four websites that did give notice, the agencies had failed to fulfill the other requirements laid out in the June 2000 OMB memo.[18]

The U.S. Congress also responded to the incident with legislation prohibiting the use of cookies in some instances. Requirements were added to the FY2001 Transportation Appropriations Act that prohibited any of the funds from being used "to collect, review, or create aggregate lists that include personally identifiable information relating to an individual's access to or use of a federal government Internet site" or to enter into any agreement with a third party for similar purposes.[19] Subsequent appropriation bills have included similar language.[20] While cookies do not necessarily contain personally identifiable information, this legislation unnecessarily restricts the use of cookies when a website also collects information such as name, e-mail address or IP address.

PRIVATE VS. PUBLIC SECTOR POLICY ON COOKIES

While the federal government restricts the use of persistent cookies, most commercial and many state and local government websites do not. To analyze this we review the privacy policies of the ten most popular private sector and public sector websites in the United States. The privacy policies of commercial websites generally support the use of persistent cookies whereas many federal government websites do not permit their use. The websites chosen in our report reflect the top ranked domains as indicated by Alexa Internet Inc., an Internet traffic ranking service that is a subsidiary of Amazon.com. For private sector websites, the report evaluates the top ten commercial domains for the United States. For public sector websites, the report evaluates the top ten U.S. federal government domains based on global web traffic statistics.[21]

Private Sector

The top ten private sector websites are: Google.com, Yahoo.com, Facebook.com, YouTube.com, MySpace.com, MSN.com, Live.com, Wikipedia.org, Craigslist.org and eBay.com. As shown in Figure 1, the privacy policies of these websites all permit the use of persistent cookies, either explicitly or implicitly. Some privacy policies provide more detail than others. For example, the privacy policy on Facebook.com states that "By default, we use a persistent cookie that stores your login ID (but not your password) to make it easier for you to login when you come back to Facebook."[22] The privacy policy on Google.com gives more detail and explains that "like most web sites and search engines, Google uses cookies in order to provide services and advertising to our users, and to improve the user experience. Cookies record users' preferences, like whether they want their results in English or French, and if they've selected a safe search filter. Without them, Google wouldn't be able to remember what different people like."[23] The privacy policy on Craigslist.org provides no detail on the use of persistent cookies merely stating "We don't employ tracking devices for marketing purposes."[24] The website does use persistent cookies to store user preferences, such as preferred language and location. Of the websites reviewed, all except YouTube.com, Wikipedia.org and Craigslist.org remind users that they have the option to control the use of cookies in their web browser.[25] Only Wikipedia.org provided detail on the maximum lifespan of a persistent cookie.

The widespread use of persistent cookies in the private sector is not surprising. As early as 1997, researchers noted a steady upward trend in the number of popular websites using persistent cookies.[26] In June 1997, 24 of the most popular 100 websites used persistent cookies; by December 1997 this number had risen to 30.[27]

FIGURE 1: USE OF PERSISTENT COOKIES ON PRIVATE SECTOR WEBSITES

	Domain	Permit Persistent Cookies?
1	Google.com	Yes
2	Yahoo.com	Yes
3	Facebook.com	Yes
4	YouTube.com	Yes
5	MySpace.com	Yes
6	MSN.com	Yes
7	Live.com	Yes
8	Wikipedia.org	Yes
9	Craigslist.org	Yes
10	eBay.com	Yes

Public Sector

This section reviews the privacy policies of the following public sector websites: USPS.com, NIH.gov, IRS.gov, NASA.gov, NOAA.gov, Weather.gov, Ed.gov, CDC.gov, State.gov, and USGS.gov. As shown in Figure 2, four out of ten of the privacy policies of the top ten ranked federal government websites permit the use of persistent cookies, either explicitly or implicitly.

Four of the websites reviewed permit the use of persistent cookies: USPS.com (United States Postal Service), NIH.gov (National Institute of Health), NASA.gov (National Aeronautics and Space Administration) and CDC.gov (Centers for Disease Control and Prevention). USPS.com allows persistent cookies for various purposes including site usage management, user session management, website personalization and ad banners. The USPS privacy policy provides detail on the various purposes of persistent cookies and the maximum lifespan of each cookie. The lifespan of a cookie created by USPS.com ranges from fifteen minutes to five years.[28] NIH uses persistent cookies to implement the American Customer Satisfaction Index, an online survey of users. The privacy policy states the purpose of using persistent cookies and defines the maximum lifespan of a persistent cookie (90 days).[29] The privacy policy on NASA.gov allows the use of persistent cookies for providing website customization. The policy does not define a maximum lifespan for persistent cookies.[30] Finally, CDC.gov allows persistent cookies but does not define the purpose or lifespan of these cookies.[31]

Some of the websites that do not permit the use of persistent cookies use clear and unambiguous language, such as IRS.gov which plainly states in its website privacy policy "The IRS does not use 'persistent cookies' or other technology to collect personally identifiable information about visitors to our Web site."[32] NOAA.gov and Weather.gov also clearly state in their respective privacy policies that their websites do not use persistent cookies. Both Ed.gov and USGS.gov do not appear to allow persistent cookies by their privacy policies, but the text is less clear. State.gov has the least precise website privacy policy and makes no specific mention of cookies in any form, yet the policy indicates that such technology would not likely be permitted.

FIGURE 2: USE OF PERSISTENT COOKIES ON FEDERAL GOVERNMENT WEBSITES

	Domain	Permit Persistent Cookies?
1	USPS.com	Yes
2	NIH.gov	Yes
3	IRS.gov	No
4	NASA.gov	Yes
5	NOAA.gov	No
6	Weather.gov	No
7	Ed.gov	No
8	CDC.gov	Yes
9	State.gov	No
10	USGS.gov	No

Finally, while we don't systematically review the use of cookies on state government websites, it appears that many state government websites use persistent cookies to improve the end-user experience. Cookies are required for some functionality, and as explained in the privacy policy on Google.com, without them, users may lose some functionality.[33] For example, the official state websites of both Michigan and Idaho, ranked first and second respectively by the 2006 National Policy Research Council report on e-government, use persistent cookies.[34] Michigan's state website uses persistent cookies to recognize returning users and customize the website content based on user preferences.[35] The State of Idaho also uses persistent cookies on its website to build more robust online applications. For example, because of the use of persistent cookies a resident applying for an online license can resume an existing application without losing any data even if the session is interrupted.[36]

GOVERNMENT WEBSITES NOT ALWAYS THE PRIMARY SOURCE OF GOVERNMENT DATA

While the Internet has created the opportunity for unprecedented transparency and openness in government, government websites are not always the primary source for government data. Some researchers have called on government to leave the task of presenting online information to the private sector arguing that it "would be preferable for government to understand providing reusable data, rather than providing Web sites, as the core of its online publishing responsibility."[37] Likewise, ITIF has argued that "Governments can move beyond engaging with the private sector as e-government vendors and instead empower third-party, for-profit and nonprofit organizations as partners in the provision of e-government services."[38] This theme has been accepted by the current administration which currently plans to develop the website data.gov with structured government data.

Even today, private sector for-profit and nonprofit organizations increasingly provide important online resources for citizens to access government data. As shown in Figure 3, some of the most popular websites for accessing government data are neither owned nor operated by the government. For example, OpenSecrets.org, a website that provides online tools to search campaign finance data, is vastly more popular than the website of the Federal Election Commission (FEC.gov) which is the primary source for this data. Or consider Fedspending.org, a website dedicated to providing transparency in government spending and sponsored by the nonprofit organization OMB Watch. Fedspending.org ranks higher than its rival government website USAspending.gov and also appears more popular with a greater number of incoming website links.

The trend of private-sector websites playing a greater role in providing access to government data also has important policy implications. If citizens decreasingly use government websites to access government data, then the privacy policies of these government websites is of less importance. Of growing importance for citizens concerned with privacy is the privacy policy of the competing private-sector websites. Privacy policies on the competing private-sector websites tend to have less restrictive privacy policies. For example, as shown in Figure 3, OpenSecrets.org uses cookies to customize access to the website but FEC.gov restricts

FIGURE 3: COMPARISON OF THE POPULARITY OF GOVERNMENT WEBSITES VERSUS COMPETING PRIVATE-SECTOR WEBSITES[39]

Purpose	Website Domain	Alexa Rank	Incoming Links	Privacy Policy
Campaign Finance Data	FEC.gov	210,077	2,574	Restricts all cookies
	OpenSecrets.org	44,472	4,060	No privacy policy. Uses persistent cookies.
Stimulus Spending	Recovery.org	12,517	404	Permits session cookies. Permits thrid party persistent cookies for video statistics.
	Recovery.gov	250,161	258	Permits cookies.
Legislation[40]	LOC.gov[41]	2,922	20,714	Permits cookies.
	Govtrack.us	30,285	3,079	No privacy policy. Uses persistent cookies.
Government Spending	USAspending.gov	303,303	315	Privacy policy does not specify. Does not appear to use cookies.
	Fedspending.org	216,825	317	No privacy policy. Does not appear to use cookies.

the use of all cookies. In addition, some of these non-governmental websites lack a privacy policy.

However, the privacy policies of websites, and specifically the use of persistent cookies, does not seem to be a factor in the popularity of websites for government data. Instead, factors such as usability and functionality likely drive user preference. Thus even if government organizations like the White House cease using third-parties like YouTube to host official government videos, it is likely that citizens will repost any official videos on such websites, and these third-party websites will be the primary venue for citizens to access this government information.

POLICY DISCUSSION AND RECOMMENDATIONS

The current federal policy is a significant factor in the limited use of persistent cookies on federal government websites. The criteria established in the June 2000 OMB memo, particularly the requirement prohibiting the use of cookies without the personal approval by the head of the agency, strictly limits the use of persistent cookies. Without persistent cookies, government agencies cannot implement many of the common features the public has come to expect on websites, such as personalization. As more content is digitized, tools to personalize and customize websites are an effective way to prevent information overload and help citizens find the information they seek. However, customization so that a website can "remember" a user often requires the use of persistent cookies. In addition, Web 2.0 technologies that can help government engage with citizens, such as Facebook and YouTube, routinely require the use of persistent cookies. Finally, government agencies cannot implement advanced web analytics, such as those to track return visitors, without persistent cookies. None of these uses of cookies present a threat to user privacy, and thus should be permitted by the federal government.

Others have also noted the need to update government regulations to provide federal agencies more flexibility to develop online content. For example, Karen Evans, the former Administrator for Electronic Government and Information Technology at OMB recently testified on the need for reform of the laws, regulations and procurement rules governing government websites. She acknowledged that the current restrictions on the use of persistent cookies prevent the use of various Internet applications that government should be embracing.[42] Members of the Federal Web Managers Council, an interagency group of senior web managers in the federal government, have similarly argued that OMB should "immediately rescind its previous guidance prohibiting persistent cookies."[43]

The Obama adminstration has already experienced the limitations of the existing policy. Privacy advocates criticized the Obama administration for embedding YouTube videos on the White House website. Embedding the videos in the government website violated the privacy policy of whitehouse.gov because YouTube sets a third-party persistent cookie. In response, the administration modified the website so visitors must first click a graphic to load the video player which sets the cookie.[44] In addition, the administration issued a waiver allowing for the use of persistent cookies in this instance and modified its privacy policy. The privacy policy acknowledges that the website may not be fully compliant with the policy in regards to the use of persistent cookies and states "we intend, however, to fully enforce the above provisions as soon as possible."[45]

The new administration has created the first Federal Chief Information Officer (CIO). Among other duties, the Federal CIO has responsibility for directing the policy and strategy of federal information technology investments and ensuring privacy across the federal government.[46] However, as others have noted, a CIO can be conflicted when tasked with both improving the flow of information and ensuring the privacy of data.[47] The Federal CIO should seek to balance privacy against other equally important goals for e-government such as usability, accessibility and transparency.

Government agencies need flexible policies that allow them to quickly and efficiently implement new online applications and services without unnecessary restrictions on the use of particular Internet technologies. **Toward that end we recommend that:**

- **The Federal CIO should direct OMB to allow the use of persistent cookies on government websites.**
- **In addition, OMB should be instructed to publish regularly updated guidelines outlining permitted uses of persistent cookies and guidance on best practices, such as specifying the maximum lifespan of persistent cookies.**
- **The Federal CIO should also work to standardize the language used in website privacy policies across government agencies.** Privacy policies should provide clear and unambiguous language to specify the activities permitted and restricted by the website.

Academics must also recognize that good privacy practices cannot be reduced to whether a website uses a certain type of technology. Unfortunately, some researchers still consider the use of cookies to be a sign of weak online privacy protections. Darrell West at the Brookings Institution has reviewed and ranked numerous government websites. However, his methodology unfairly penalizes government websites for the use of cookies. As explained in a 2008 report on state and federal government websites, he writes "53 percent of government websites prohibited the commercial marketing of visitor information. Forty percent prohibited the use of cookies or individual profiles."[48] Researchers should not penalize government agencies for such practices, as it will serve as a disincentive for change.

Without persistent cookies, government agencies cannot implement many of the common features the public has come to expect on websites, such as personalization.

Given the widespread use of persistent cookies in the private sector, the restrictive federal government regulations on the use of persistent cookies are antiquated. Federal regulations for government websites should emphasize privacy; however, privacy should not be emphasized at the expense of other laudable goals for e-government such as usability, transparency and accessibility. While government agencies may not always be the best organization to present data online, agencies need flexible regulations to quickly implement new technology, including those using cookies.[49] Used properly, cookies pose no threat to online privacy. Moreover consumers today have much choice among Internet browsers, and every major web browser includes many features to allow users control over their online privacy and the use of cookies. In other words, citizens now have tools to ensure that online interactions with government occur on their own terms. Rather than restrict specific technology such as cookies, government regulations should instead focus on protecting civil liberties through continued government oversight on the collection and use of personally identifiable information.

CONCLUSION

In an ever-changing world, government must always be willing to change and adapt policies to new situations and circumstances. In particular, rapid developments and progress with technology necessitate flexible government policies that do not hindier technological progress. As President Obama stated recently in his call for reforming government, "…we must also recognize that we cannot meet the challenges of today with old habits and stale thinking. So much of our government was built to deal with different challenges from a different era."[50] The same idea holds true for e-government.

ENDNOTES

1. Other similar technologies, such as web beacons (AKA “web bugs” or “tracking pixels”) and Flash cookies (AKA “local shared objects”) have also been criticized by some privacy advocates.

2. Data from author experiments on May 11, 2009.

3. Cookies enable a stateful web browsing experiences over HTTP—a stateless protocol.

4. Technically the cookie has an expiration date, but this can be set to a date beyond the expected lifespan of the computer.

5. “DART Ad-Serving and Search Cookie Opt-Out,” DoubleClick.com <www.doubleclick.com/privacy/dart_adserving.aspx> (accessed May 11, 2009).

6. “Opt Out of Behavioral Advertising,” Network Advertising Initiative (NAI) <www.networkadvertising.org/managing/opt_out.asp> (accessed May 11, 2009).

7. “Privacy Policies on Federal Web Sites,” Memorandum from Jacob J. Lew to the heads of executive departments and agencies, June 2, 1999 <www.whitehouse.gov/omb/memoranda/m99-18.html> (accessed May 11, 2009).

8. “M-99-18 Attachment: Guidance and Model Language for Federal Web Site Privacy Policies,” Office of Management and Budget, June 1, 1999 <www.whitehouse.gov/omb/memoranda/m99-18attach.html> (accessed May 11, 2009).

9. Marcia S. Smith et al., “Internet: An Overview of Key Technology Policy Issues Affecting Its Use and Growth” Congressional Research Service, January 31, 2001.

10. Not to be confused with the Cookiegate saga of 2008 when Cindy McCain, spouse of Republican Presidential nominee Senator John McCain, allegedly submitted an oatmeal-butterscotch cookie recipe that came from Hersheys.com to a magazine contest.

11. “Privacy Advocates Call on Congress to Investigate ‘Cookiegate,’” Electronic Privacy Information Center, press release, June 22, 2000 <epic.org/privacy/internet/cookiegate_pr.html> (accessed May 11, 2009).

12. “Privacy in the Information Age, Part 1: Internet Privacy,” The Forum on Technology & Innovation. Transcript, April 26, 2000 <www.tech-forum.org/upcoming/transcripts/IntPrivTrans_04-26-00.htm> (accessed May 12, 2009).

13. Duncan Graham-Rowe, “Europe may ban internet cookies,” New Scientist, November 1, 2001 <www.newscientist.com/article/dn1509-europe-may-ban-internet-co> (accessed May 12, 2009).

14. “M-00-13: Privacy Policies and Data Collection on Federal Web Sites,” Office of Management and Budget, June 22, 2000 <www.whitehouse.gov/omb/memoranda/m00-13.html> (accessed May 11, 2009).

15. Letter from Roger W. Baker to John T. Spotila, July 28, 2000 <www.whitehouse.gov/omb/inforeg_cookies_letter72800/> (accessed May 11, 2009).

16. Letter from John T. Spotila to Roger W. Baker, September 5, 2000 <www.whitehouse.gov/omb/inforeg_cookies_letter90500/> (accessed May 11, 2009).

17. Linda D. Koontz, “GAO-01-147R Federal Agency Use of Cookies,” Government Accountability Office, October, 20 2000.

18. “GAO-01-424: Implementation of Federal Guidance for Agency Use of ‘Cookies,’” Government Accountability Office, April 2001.

19. “Public Law 106-346, 106th Congress,” Government Printing Office <frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ346.106> (accessed May 11, 2009).

[20] Marcia S. Smith, “Internet Privacy: Overview and Pending Legislation,” Congressional Research Service, Library of Congress, October 2005.

[21] Alexa explains its ranking method as follows: Alexa’s traffic rankings are based on the usage patterns of Alexa Toolbar users and data collected from other, diverse sources over a rolling 3 month period. A site’s ranking is based on a combined measure of reach and pageviews. Reach is determined by the number of unique Alexa users who visit a site on a given day. Pageviews are the total number of Alexa user URL requests for a site. However, multiple requests for the same URL on the same day by the same user are counted as a single pageview. “Frequently Asked Questions,” Alexa Internet Inc. <www.alexa.com/help> (accessed May 11, 2009).

[22] “Facebook’s Privacy Policy,” Facebook <www.facebook.com/policy.php> (accessed May 11, 2009).

[23] “Privacy FAQ,” Google Inc., n.d. <www.google.com/intl/en/privacy_faq.html#toc-cookies> (accessed May 11, 2009).

[24] “Privacy Policy,” Craigslist, n.d. <www.craigslist.org/about/privacy_policy> (accessed May 11, 2009).

[25] The privacy policy on MySpace.com technically states “You can program your computer to warn you each time a cookie is being sent, block third party cookies or block all cookies.” See “Privacy Policy,” MySpace.com, n.d. <www.myspace.com/index.cfm?fuseaction=misc.privacy> (accessed May 11, 2009).

[26] Bill Helling, “Web-Site Sensitivity to Privacy Concerns: Collecting Personally Identifiable Information and Passing Persistent Cookies,” First Monday (February 1998) Vol. 3, no. 2. and “Surfer Beware” <www.epic.org/reports/surfer-beware.html> (accessed May 11, 2009).

[27] Ibid.

[28] “Privacy Policy,” United States Postal Service, n.d. <www.usps.com/privacyoffice/privacypolicy.htm> (accessed May 11, 2009).

[29] “Persistent Cookies and the American Customer Satisfaction Index,” National Institute of Health, U.S. Department of Health and Human Services, June 25, 2008 <nih.gov/about/acsi.htm> (accessed May 11, 2009).

[30] “NASA Web Privacy Policy and Important Notices,” NASA <www.nasa.gov/about/highlights/HP_Privacy.html> (accessed May 11, 2009).

[31] “Privacy Policy Notice,” CDC <www.cdc.gov/doc.do?id=0900f3ec80093c90> (accessed May 11, 2009).

[32] “IRS Privacy Policy,” Internal Revenue Service <www.irs.gov/privacy/index.html?navmenu=menu2> (accessed May 11, 2009).

[33] “Privacy Policy,” Google Inc., op. cit.

[34] “Report Card: The Best e-government Sites,” Computerworld/National Policy Research Council (2006) <www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9005371> (accessed May 12, 2009).

[35] “Michigan Privacy Policy,” State of Michigan. n.d. <www.michigan.gov/som/0,1607,7-192-26914-2088--,00.html> (accessed May 12, 2009).

[36] “Access Idaho Privacy Policy,” State of Idaho. n.d. <www.accessidaho.org/privacy.html> (accessed May 12, 2009).

[37] David Robinson, Harlan Yu, William Zeller, and Edward W. Felten, “Government Data and the Invisible Hand,” 11 Yale Journal of Law & Technology 160 (2008) <www.yjolt.org/files/robinson-11-YJOLT-.pdf> (accessed May 12, 2009).

[38] Robert D. Atkinson, “Turbo Government: A Bold New Vision for E-government,” Information Technology and Innovation Foundation, Washington, D.C., September 27, 2006 <www.itif.org/files/turbogov.pdf> (accessed May 18, 2009).

[39] Author research, Alexa.com, May 1, 2009.

[40] Perhaps a better measure here is that Google reports 16,000 incoming links to Thomas.loc.gov versus 3,250 for Govtrack.us. Source: Author research "link:Thomas.loc.gov" versus "link:govtrack.us" on May 1, 2009.

[41] According to Alexa.com THOMAS.LOC.gov accounts for 6.2 percent of total traffic to LOC.gov. Alexa does not provide rankings for subdomains. THOMAS is the website hosted by the Library of Congress that provides access to legislative information.

[42] "Statement of Karen S. Evans, Former Administrator for Electronic Government and Information Technology, Office of the Management and Budget," Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security. Senate Committee on Homeland Security and Governmental Affairs, April 28, 2009 <hsgac.senate.gov/public/_files/TESTIMONYEVANS42809.pdf> (accessed May 12, 2009).

[43] Bev Godwin, Sheila Campbell, Jeffrey Levy and Joyce Bounds, "Social Media and the Federal Government: Perceived and Real Barriers and Potential Solutions," Members of the Federal Web Managers Council <www.usa.gov/webcontent/documents/SocialMediaFed%20Govt_BarriersPotentialSolutions.pdf> (accessed May 12, 2009).

[44] Thomas Claburn, "YouTube Denies Being 'Ditched' By White House," InformationWeek, March 3, 2009 <www.informationweek.com/news/internet/web2.0/showArticle.jhtml?articleID=215800228> (accessed May 12, 2009).

[45] "Our Online Privacy Policy," White House <www.whitehouse.gov/privacy/> (accessed May 12, 2009).

[46] "President Obama Names Vivek Kundra Chief Information Officer," The White House, Office of the Press Secretary, press release, March 5, 2009 <www.whitehouse.gov/the_press_office/President-Obama-Names-Vivek-Kundra-Chief-Information-Officer/> (accessed May 12, 2009).

[47] "CIO Council turns focus on privacy," Privacy Digest, October 25, 2007 <www.privacydigest.com/2007/10/25/cio+council+turns+focus+privacy> (accessed May 12, 2009).

[48] Darrell M. West, "State and Federal Electronic Government in the United States, 2008," (Washington, D.C.: Brookings Institution, August 26, 2008) <www.brookings.edu/~/media/Files/rc/reports/2008/0826_egovernment_west/0826_egovernment_west.pdf> (accessed May 12, 2009).

[49] Robert D. Atkinson, "Turbo Government: A Bold New Vision for E-government," op.cit.

[50] "Weekly Address: President Obama Announces Steps to Reform Government and Promote Fiscal Discipline," The White House, Office of the Press Secretary, press release, April 25, 2009 <www.whitehouse.gov/the_press_office/Weekly-Address-President-Obama-Announces-Steps-to-Reform-Government-and-Promote-Fiscal-Discipline/> (accessed May 12, 2009).

ABOUT THE AUTHOR

Daniel Castro is a Senior Analyst with ITIF. His research interests include technology policy, security, and privacy. Mr. Castro has an MS in information security technology and management from Carnegie Mellon University.

ABOUT THE INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION

The Information Technology and Innovation Foundation (ITIF) is a nonprofit, non-partisan public policy think tank committed to articulating and advancing a pro-productivity, pro-innovation and pro-technology public policy agenda internationally, in Washington and in the states. Through its research, policy proposals, and commentary, ITIF is working to advance and support public policies that boost innovation, e-transformation and productivity.

For more information contact ITIF at 202-449-1351 or at mail@itif.org, or go online to www.innovationpolicy.org.
ITIF | 1101 K St. N.W. | Suite 610 | Washington, DC 20005