Comments of the World Privacy Forum to Office of Management and Budget, Executive Office of the President

regarding

Proposed revision of the policy on web tracking technologies for federal web sites

Via email to oira_submission@omb.eop.gov

August 10, 2009

Mabel Echols
Office of Information and Regulatory Affairs,
Records Management Center,
Office of Management and Budget
Room 10102
NEOB, 725 17th Street NW
Washington, DC 20503

Re: Proposed revision of the policy on web tracking technologies for federal web sites

Thank you for the opportunity to submit comments regarding the proposed revision of the OMB policy on web tracking technologies for Federal web sites, 74 Federal Register 37062 (July 27, 2009).

The World Privacy Forum is a non-partisan, non-profit public interest research and consumer education organization. Our focus is on conducting in-depth research and analysis of privacy issues, including issues related to technology, the workplace, and health care. We have done substantial work in the area of online privacy. See <http://www.worldprivacyforum.org>.

There are numerous technical and policy issues relating to the issue of persistent identifiers and online use. These comments discuss some of these issues briefly as they relate to government web sites.

I. What does "opt out" apply to in the government context?

Setting aside for the moment the broader issue of whether an opt-out or opt-in approach is more appropriate for the U.S. Government, "opting out" has many potential meanings and applications. The Federal Register notice did not articulate specific ideas the administration may have regarding what an opt out may or may not apply to. Does an opt

out apply to mobile users? To desktop computer users? If the opt out applies to all users, then how does the opt out mechanism itself work? Will the opt out only work through a web browser?

For example, any vision of an opt-out mechanism that relies on web browsing conducted via a personal computer is far too narrow by today's standards. *Online* can mean a mobile phone or a Blackberry retrieving video, music, books, streams of text messages, or other forms of information. Video formats allow for different kinds of tracking that go beyond the traditional HTML cookie opt out. Simply put, *online* today is much broader than an individual sitting at a computer connected to the Internet.

It is difficult to imagine that a person using a mobile phone would scroll through a lengthy privacy policy to find the option to click on an opt-out cookie that would likely not work for the phone. Much work needs to be done to expose all relevant technologies and to provide appropriate consumer rights and protection. This work should be accomplished through a sincere process that precisely determines what the proposed opt out will apply to, and what mechanisms that opt out will use.

II. Will a government web opt out require user authentication?

For some opt outs, for example, those that span platforms, such as an opt out that applies to both a user's mobile phone and to the user's desktop web browsing, typically some form of authentication needs to tie the user's sessions or information together. This can, for example, come in the form of a log on or registration. So for example, would the federal government be providing a single opt out for a user who accesses *whitehouse.gov* from a mobile phone one day and from a computer the next?

If the government is contemplating a multi-platform or even a multi-platform, multi-session opt out, is the government also contemplating authenticating users? If so, then that opens up a challenging set of new issues that were not included in the Federal Register notice, issues that would need to be carefully considered separately.

The World Privacy Forum believes web visitors to government web sites should not need to undergo authentication unless they are accessing a restricted service of some sort that absolutely requires it.

If the government decides to move forward with web visitor authentication in any form, any authentication scheme should be proposed in a formal comment format, with a minimum of 30 days for commenting. Further, the government should construct any authentication plan with active and meaningful input from all members of relevant civil society groups, including the full range of privacy and civil liberties groups.

The reason authentication is an issue here is that any opt-out mechanism to prevent tracking requires some degree of tracking of the actual opt outs. The choices available to the government for online opt-out are limited, and each carries substantial drawbacks. The most significant drawback of a multi-platform opt out is the complex set of problems

associated with authentication. The most significant drawbacks of an HTML- based opt out are multiple, and deserve a separate discussion, which we have included below.

III. The government should not be contemplating relying on the broken web browser/opt-out-cookie based mechanism

Today, the term "opting out" of persistent trackers in the web context typically means that consumers will use their web browsers to download something called an opt-out cookie. The opt-out cookie is the current primary opt-out mechanism to remove the consumer from unwanted tracking by web sites. The problem is that opt-out cookies have many known problems, including a lack of longevity, among other things. If the government is planning on using an opt-out HTML- cookie-based mechanism, then it is crucial to understand that this mechanism is broken.

The Federal Register notice was non-specific about particular opt-out mechanisms the government is contemplating. Because the current cookie-based opt-out mechanism has failed, it is worth spending some time looking at why.

A. The opt-out cookie is counterintuitive for consumers

Downloading one cookie so other cookies don't track you is a message most consumers have never really heard or understood. Although the Federal Register notice stated with confidence that tracking technologies have become a "staple" on web sites and have achieved "widespread public acceptance," studies indicate that the reality is that consumer confusion exists regarding even standard uses of cookies.[1]

It is reasonable to conclude that the opt-out cookie is just one more confusing aspect of cookies for consumers, and that consumers are not clear on what the opt-out cookie does or does not do in regards to privacy protections. If the government is contemplating using an opt-out mechanism based on a cookie delivered by a web browser, the government should know that consumers are confused about cookies in general, and opt-out cookies present even more of a hurdle.

B. Opt-out cookies do not work

[1]A number of studies point to continuing consumer confusion about cookies. In particular, in a July 2007 study, InsightExpress found that "individuals who choose to delete cookies for one or more reasons possibly misunderstand the roles and functions served by cookie technology." The 2007 study found that 63 percent of respondents believed they had deleted their cookies, when only 23 percent actually had. The study was a repeat of a 2005 InsightExress study that found that of 59 percent of respondents who tried to delete cookies, only 35% of the "deleter group" studied were able to successfully delete their cookies. See *InsightExpress Study Sheds New Light on Cookie Deletion*, Business Wire, July 17 2007. See also *New Research Reveals Significant Consumer Misunderstanding of Cookies; Few Understand the Function of Cookies and Only 35% of Online Consumers are Able to Successfully Delete Them*. Business Wire, April 21, 2005. These numbers are in line with comScore's examination of approximately 400,000 U.S. users in December 2006 which found that about 31 percent of U.S. computer users clear their first-party cookies in a month, with similar numbers for clearing third party ad network cookies. See *The Impact of Cookie Deletion on the Accuracy of Site-Server and Ad-Server Metrics: An Empirical comScore Study*, comScore, June 2007. <http://www.comscore.com>.

Opt-out cookies, if they are indeed the mechanism the government contemplates using to facilitate web tracking opt outs, have a documented history of failure and are inappropriate vehicles for the government to rely on for consumer privacy.

1. Background of how opt-out cookies began

Opt out cookies were born in 1999, when widespread concerns arose about the ways that consumers could be tracked and targeted online for advertising purposes. The Federal Trade Commission held a workshop on online profiling in November 1999.[2] The concerns of the day were distilled in a FTC report to Congress in June 2000, *Online Profiling: A Report to Congress*. In that report, the FTC found that online profiling presented privacy problems for consumers. The FTC found that online profiling was primarily accomplished through banner ads, cookies, and web bugs, also called web beacons.[3] The Commission also concluded that online profiling was largely invisible to consumers:

> Although network advertisers and their profiling activities are nearly ubiquitous, they are most often invisible to consumers. All that consumers see are the Web sites they visit; banner ads appear as a seamless, integral part of the Web page on which they appear and cookies are placed without any notice to consumers. Unless the Web sites visited by consumers provide notice of the ad network's presence and data collection, consumers may be totally unaware that their activities online are being monitored.[4]

In the spring of 1999, prior to its November workshop, the FTC invited network advertising companies to "discuss business practices and the possibility of self-regulation."[5] The companies announced the formation of the NAI, or the Network Advertising Initiative, at the 1999 November workshop. These self-regulatory efforts were discussed in the first FTC report to Congress, which was published in June 2000.[6]

The Senate Commerce Committee held hearings on online profiling in June 2000. At that time, the Committee heard that privacy and consumer rights groups had not been involved in the industry discussions, with the consequence that a week later, seven senators on the Committee wrote urging the FTC to include privacy and consumer groups in the talks. Some groups were invited to examine a mock up of the final NAI agreement on July 19.[7] On July 27, the final agreement was released publicly in its final form in the

---

[2] A transcript of the Workshop is available at <http://www.ftc.gov/bcp/profiling/index.htm>.

[3] *Online Profiling: A Report to Congress*, pages 2-3. "In general, these network advertising companies do not merely supply banner ads; they also gather data about the consumers who view their ads. This is accomplished primarily by the use of "cookies"11 and "Web bugs" which track the individual's actions on the Web." < http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf>.

[4] *Id*. at 6.

[5] *Id*. at 22.

[6] *Id*. at 22.

[7] For more about the lead-up to the final publication of the NAI agreement, see *Network Advertising Initiative: Principles not Privacy*, July 2000, EPIC and Junkbusters. <http://www.epic.org> and

FTC's second report to Congress on online profiling (July, 2000). In this report, the FTC recommended the NAI as a self-regulatory solution to the problem of online profiling of consumers.

> The Commission commends the NAI companies for the innovative aspects of their proposal and for their willingness to adopt and follow these self-regulatory principles. Their principles address the privacy concerns consumers have about online profiling and are consistent with fair information practices. As the Commission has previously recognized, self-regulation is an important and powerful mechanism for protecting consumers, and the NAI principles present a solid self-regulatory scheme. Moreover, NAI members have agreed to begin to put their principles into effect immediately while Congress considers the Commission's recommendations concerning online profiling.[8]

The FTC also noted in its second report that legislation was needed to bolster the NAI:

> Nonetheless, backstop legislation addressing online profiling is still required to fully ensure that consumers' privacy is protected online. For while NAI's current membership constitutes over 90% of the network advertising industry in terms of revenue and ads served, only legislation can compel the remaining 10% of the industry to comply with fair information practice principles. Self-regulation cannot address recalcitrant and bad actors, new entrants to the market, and drop-outs from the self-regulatory program. In addition, there are unavoidable gaps in the network advertising companies' ability to require host Web sites to post notices about profiling, namely Web sites that do not directly contract with the network advertisers; only legislation can guarantee that notice and choice are always provided in the place and at the time consumers need them.[9]

The NAI was never debated publicly in any robust or formal manner. Nine network advertising companies signed the NAI founding document.[10]

Ultimately, the essential activity of the NAI is to define terms, discuss a handful of abbreviated consumer rights, which the NAI calls its "principles," and to set up a structure of "opt-out cookies." That structure of opt-out cookies is still in place, and it has been famously ineffective.

2. Effectiveness of opt-out cookies: by the numbers

Some of the questions the government needs to ask about opt-out cookies relates to how effective – or not – they have been in the private sector over the past ten years. These questions need to be answered before any cookie-based opt-out regime is considered.

<http://www.junkbusters.com>. "Privacy and consumer groups were not allowed to retain or distribute any of the documents discussed."

[8] Federal Trade Commission. *Online Profiling: A Report to Congress Part 2 Recommendations*, July 2000. < http://www.ftc.gov/os/2000/07/onlineprofiling.pdf> at 9.

[9] *Id* at 10.

[10] The original NAI members were 24/7 media, AdForce, AdKnowledge, Avenue A, Burst Media, Doubleclick, Engage, L90, and Matchlogic. See *Network Advertising Initiative, Self-regulatory Principles for Online Preference Marketing by Network Advertisers*, July 10, 2000.

What do we know about:

- How effective have opt-out cookies been?
- How many consumers know about opt-out cookies?
- How many consumers understand opt-out cookies?
- How many consumers have downloaded opt-out cookies?
- How long do most consumers keep opt-out cookies?
- How has industry made consumers aware of opt-out cookies, and how effective has that been?
- Do HTML opt-out cookies prevent online consumer tracking?

The answers to many of these questions are already known by the network advertisers who have been using opt-out cookies for a decade now through the NAI agreement, and who generally keep excellent track of their cookies.

TRUSTe, the current enforcer of the NAI agreement, used to report on NAI complaints about opt-out cookies. In March 2002, TRUSTe's first report on NAI enforcement documented that there were 30 complaints about the NAI, and every one of the complaints was about opt-out cookies. Complaints about opt-out cookies continued all the way through December 2004, the last month that TRUSTe reported opt-out cookie complaints publicly. It is unknown how many consumers are still complaining about opt-out cookies, as there is no longer any public reporting on them from TRUSTe. But even the limited TRUSTe reports that are available are revealing.

The Network Advertising Initiative, in public comments filed with the FTC in October 2007, said that in 2001, the NAI web site was visited 30,000 times during its first week of operation.[11] NAI also commented that: "…in 2006 we estimate that our opt-out page was visited 1,003,750 times." It is unknown if these were unique visitors, and it is unknown how many of those visitors opted-out successfully. It is also unknown what percentage of visitors to the opt-out site this constitutes compared to the universe of consumers who have had behaviorally-targeted network ads served to them.[12]

3. Current cookie-based opt-out regimes are impressively difficult for consumers

It is far from clear that any form of an opt-out cookie should be the mechanism of first choice for consumer protection from web tracking, given all of the demonstrated difficulties with cookie-based opt-out regimes that are currently in place.

---

[11] Public Comments of the Network Advertising Initiative, *Network Advertising (NAI) Written Comments for the FTC's Ehavioral Advertising Town Hall Forum*, October 19, 2007. <http://www.ftc.gov/os/comments/behavioraladvertising/071019nai.pdf>.

[12] The privacy policy on the NAI website says that NAI becomes the "sole owner of all information collected on this site." If a consumer who is confused about an opt-out cookie fills out an NAI "contact us" form, the privacy policy language suggests that NAI becomes the "sole owner" of the consumer's name, email address, and other information. It isn't clear whether the statement in the privacy policy has any real meaning or effect, but it is an example of where a self-regulatory body has not adequately thought through the consumer perspective of the process. <http://www.networkadvertising.org/about/privacy.asp>.

Opting out is hard to do, and generally clunky from web browsers. For example, those seeking to opt-out of tracking by NAI members must visit <www.networkadvertising.org> with cookies turned on. After landing on the home page, consumers who click the opt-out button on the page are sent to the NAI opt-out page. The page offers checkboxes that correlate to an opt-out for different NAI members. Each check box should result in the setting of a separate opt-out cookie on the consumer's computer. However, the results are highly variable, and the opt-outs often are not successfully set.

In a series of tests using different computers, IP addresses, browser types, and operating systems, the World Privacy Forum tested how well the official NAI opt-out page was working.[13]

The Forum also invited others to opt-out and report on their experiences. One individual who tried to opt-out sent in a pithy note: "It didn't work so well" accompanied by a screen shot of the results of his opt-out effort. The screen shot revealed that only two of the opt-outs on the page had actually worked for this consumer.[14]

World Privacy Forum tests demonstrated that opt-outs on the NAI page do not always work even when browsers are optimally set to accept all cookies. Even when different kinds of web browsers were set to accept all cookies, the opt-out cookies were not always set properly. It is difficult to offer a hard number for the failure rate for setting NAI opt-out cookies due to the high variability in the causes for failure. However, for some standard computer operating systems and browsers, the failure rate exceeds 50 percent, depending on the computer set-up, firewall settings, and many other factors.

For example, in one test run, using computers running Firefox or IE on MS Windows and Safari on Mac OSX, World Privacy Forum tests found that checking the multiple opt-out boxes offered by NAI resulted in only some NAI opt-out cookies being set successfully. (The NAI opt-out page has a feature that tells users whether the opt-out was successful or not.) Using a computer running Mozilla on a SUN Ultra, and a computer running Firefox on Mac OSX, one test found that the opt-out worked. However, firewall settings can influence these results, so there is high variability of opt-out success or non-success.

The NAI opt-out page titled "Having Trouble Opting Out?" addresses these issues and says:

> The performance of the global opt-out tool might be affected by a number of factors outside the control of the NAI and/or its member ad networks. These factors include corporate network security, telecommunications breakdowns,

[13] The page the WPF tested was <http://www.networkadvertising.org/managing/opt_out.asp>.
[14] The email is on file at the WPF offices and is available, but is only available redacted of personally identifiable information about the consumer.

> browser settings, ISP or infrastructure anomalies and client-side technical glitches, among other possible issues.[15]

The NAI is well aware of the problems with the opt-outs. In its public comments to the FTC in October 2007, the NAI wrote:

> The single most common issue raised by consumers about the NAI Principles program relates to the functionality of the opt-out. It is rather common for consumers to request assistance to ensure that their opt-out cookie is functioning properly (browser compatibility concerns). The vast majority of these concerns are successfully addressed by having a staff member work directly with the consumer to resolve the problem they had been experiencing.[16]

It would be helpful to know how often consumers spoke to or communicated with NAI staff, and the specific results of those contacts.

Given the large variety of computer types, machine configurations, corporate and personal firewall configurations, web browsers and browser configurations, the government will have its hands full trying to help consumers opt-out should it go this direction.

4. Cookie-based opt-outs are susceptible to deletion

Opt-out cookies only work when they have been downloaded to a user's hard drive and stay there. Opt-out cookies may be deleted by users who delete all of their cookies at one time, no matter what kind of cookies they are. Several studies have reliably shown that about 30 percent of consumers delete cookies.[17] Consumers who run a security protection program that removes spyware and malware may inadvertently erase opt-out cookies. Some consumers operate these programs as a standard part of their computer hygiene routine.

Unless a consumer is highly knowledgeable about cookies and is able to distinguish opt-out cookies from other cookies, consumers may not be able to maintain their opt-out cookies over time. These problems with reliance on opt-out cookies are not new, and they have been known for many years.

5. A cookie-based opt-out does not touch all of the other persistent identifiers and trackers

A traditional HTML cookie is not the only persistent identifier and tracker available anymore. New technologies and techniques have become routine business practice,

---

[15] NetworkAdvertising.org < http://www.networkadvertising.org/managing/optout_problems.asp>.See also < http://www.networkadvertising.org/managing/faqs.asp#question_16>.

[16] Public Comments of the Network Advertising Initiative, FTC, October 19, 2007. <http://www.ftc.gov/os/comments/behavioraladvertising/071019nai.pdf>.

[17] See *supra* note 27.

particularly in the area of persistent identifiers and tracking technologies. A rich array of browser cache cookies, Flash cookies, DOM cookies and other techniques exist.

The non-HTML based persistent identifiers and trackers are particularly important in connection with the government's allowance of consumer tracking by third parties, and will be discussed more below.

IV. Third-party tracking is not appropriate on government web sites

The Federal Register notice contemplates a three-tiered approach to the use of Web tracking technologies on government web sites, mentioning web analytics as a primary reason for this. But the notice largely sidesteps the broader issue of allowing third parties to track visitors to government web sites. The World Privacy Forum argues against allowing third party tracking of US government web site users.

First, third party tracking is unnecessary.

Second, any government opt-out mechanism that is intended to stop third-party tracking and is based on standard HTML cookies may be circumvented by non-HTML tracking mechanisms. We again note that a traditional HTML cookie is not the only persistent identifier and tracker available anymore. What will the government's opt out be? If it is a standard HTML cookie, then third parties using browser cache cookies, Flash cookies, DOM cookies and other technologies can track those users despite an active a government HTML-based opt out sitting on a user's hard drive.

Briefly, for background, here are some persistent trackers other than HTML cookies; these tracking mechanisms are not considered to be exotic or rare, and some are in widespread use:

Browser cache cookies:

The browser cache cookie is a semi-persistent tracker.[18] A browser cache cookie loads a persistent identifier into the browser cache area of a consumer's computer. Very few, if any, consumers know to clear out their browser cache to remove persistent identifiers. Several patents and or patent applications exist in the area of browser cache cookies, and there are a number of known variations of browser cache-based tracking techniques. One patent application discusses browser cache cookies as "secret cache cookies."[19]

Flash cookies:

While it was never intended as a persistent tracking device, the Adobe Flash[20] program's Local Shared Objects (LSO) function allows the storage of persistent unique identifiers

[18] Technical note: In this discussion, a browser cache cookie means the eTag and similar techniques.

[19] Jakobsson; Bjorn Markus; et al, US Patent Application 20070106748. May 10, 2007 at 16, 17, 19.

[20] >http://www.adobe.com/products/flash/>.

from third parties.[21] Nicknamed "Flash cookies," or "third party Flash cookies," these tracking files reside in a folder outside of the traditional cookies folder that users work with in most browsers.[22] Flash cookies function similarly to cookies in terms of their tracking capabilities.

Flash cookies are not identical to traditional cookies. They are stored in a different area than a traditional cookie, and Flash cookies have a much larger capacity for storage.[23] Although most companies use Flash cookies to simply store a numeric identifier that links back to a server (similar to a traditional cookie), it is possible for a company to store more information in the Flash cookie file. Adobe itself notes that *third party* local shared objects have implications for privacy and for tracking that users need to be concerned about:

> A *third-party local shared object*, sometimes referred to as a "third-party Flash cookie," is a shared object created by third-party content, or content that is not actually located on the site you are currently viewing. Third-party local shared objects may be important for privacy discussions because they can be used to track your preferences or your website usage across different websites that you visit.[24]

Adobe has a web site that allows users to set the LSO folder in ways that can include rejecting flash cookies altogether.[25] However, most users do not know about Flash cookies, and even fewer know how to manage or disable Flash cookies.

The government's proposal is silent about technologies like Flash cookies. A traditional HTML opt-out cookie, if downloaded, would not disable tracking that uses third party Flash cookies. Some have estimated that 98 percent of computers have Flash and therefore the ability to store Flash cookies.[26] Even if an individual opted out of tracking, the government or a third party could deposit a third party Flash cookie or LSO with a tracking number. The effect could be the same or similar as third party tracking cookies.

Flash cookies point up yet again the deficiencies of depending on HTML opt-out cookies for opting out of tracking. Given the popularity of video and video ads, this deficiency is

---

[21] There is also the capacity of Remote Shared Objects, which appear to be rarely used. RSOs function similarly to LSOs. See note 34.

[22] We note that there are Flash cookie and browser cache cookie plug-ins available for Firefox that will delete these kinds of cookies. But these tools require two separate downloads, and are not built directly into the browser. This means more consumer education, and more consumer steps.

[23] Adobe Tech Note: What is a local shared object? <http://kb.adobe.com/selfservice/viewContent.do?externalId=tn_16194&sliceId=1>.

[24] *Id*.

[25] The Adobe Flash preference manager is available at "How to manage and disable Local Shared Objects": <http://kb.adobe.com/selfservice/viewContent.do?externalId=52697ee8&sliceId=1>. There is a demo available that gives step-by-step advice on how to restrict Flash cookies.

[26] Matt Marshall, *New cookies, with PIE, are harder to throw out*. Sunday Gazette-Mail, Charleston, W.V. May 1, 2005.

potentially substantial. We note in passing that some government sites already allow third- party Flash cookies to be deposited.

V. Notice does not equal privacy protection

The Federal Register notice indicates a focus on the notion of "clear and conspicuous" notice on each web site regarding tracking technologies. Clear and conspicuous notice is not the same as good privacy practices. A notice to consumers, even if 100 percent perfectly articulated, posted, and understood, is not a substitute for adequate consumer protection and appropriately-crafted policies that actually protect consumers.

Notice is good, and it is a part of Fair Information Practices. But notice alone is not enough, and notice can be deeply flawed for a number of reasons. For example, notices can be incomplete. A number of web sites do not notify consumers of the use of Flash cookies – and as already discussed, Flash cookies can be used as a type of persistent identifier. Users should be informed of the presence of these persistent identifiers, and should be given the option of removing them if they so choose.

Notices, even the best ones, can also be misunderstood. Multiple studies have found problems with consumer understanding of privacy notices. One study found that consumers, when they see the words "privacy policy," expect that their information will not be shared.[27] This suggests that many consumers will have difficulty fully understanding privacy and cookie functions in a meaningful way, even if given clear and conspicuous notice. This argues against the government ever moving to allowing third party tracking of the use of government web sites, even if there is robust notice.

VI. Discrimination against those who opt-out

The Federal Register notice makes a qualifying statement about discrimination and those who "opt out," stating that those users who opt out will not be discriminated against "in terms of their access to information." This appears to stipulate a requirement for ensuring the lack of discrimination in only one discrete area, where in fact many potential areas for discrimination exist. No discrimination *whatsoever* should be occurring to any individual who chooses to opt out, whether that be in access to information or any other potential use or application of information.

Further, an opt-out regime is contemplated as a given in the discussion of non-discrimination policy. The government should not be basing its policies on a defacto reliance on opt-out, especially when web opt-out mechanisms have been proven to be problematic over the last decade. It is possible to make a sound argument that opt-out policies themselves can discriminate against individuals with less computer skill and access to technology, as opting out can be challenging for even experienced users.

---

[27] See Research Report: *Consumers Fundamentally Misunderstand the Online Advertising Marketplace*, Joseph Turow, Deirdre K. Mulligan, Chris Jay Hoofnagle. University of Pennsylvania Annenberg School for Communication and UC-Berkeley Law's Samuelson Law, Technology & Public Policy Clinic.

The government has a great deal of work to do to ensure that discrimination does not take place.

VII. Questions

We have already noted that specific forms of opt out were not mentioned. The Federal Register notice also did not discuss several other important areas, that is, data retention by third parties, secondary use of data, and user consent.

Data retention is set to become a difficult area due to competing government interests. To mitigate privacy issues, data retention must be kept to a strict minimum. But we note that cybersecurity concerns within government will argue for maximum data retention. This is a problem area, and based on past experience, it is likely that cybersecurity concerns will win the argument.

Another difficult area is secondary use of individually identifiable data, aggregate data, or general behavioral data on government web site users by parties other than the government, or by government agencies the user did not knowingly interact with. In the commercial sector, the acquisition of user consent is often proposed as an answer to secondary use problems. We have found consent to be highly challenging in an online environment, and caution against a reliance on consent for privacy protection, especially by the U.S. government.

That being said, the greater issue of secondary use is a substantial one that will have to be tackled in this context regardless of the existence of consent. Secondary use of data is highly problematic for government web sites given the sensitive nature of much of the data the government is in a position to hold and to receive via the web. Health data and support and research for health conditions, drugs, and so forth are just one area among the thousands that exist in the government web realm.

VIII. Federal Register notice and comment period

We appreciate the Federal Register notice for this Request for Comments. However, any future request for public input to this program should be given the full 30-day notice period at the minimum. We note that the comment period for this notice was short, and occurred in the middle of the summer. We believe this may have prevented some interested parties from submitting comments.

Given that this program stands to potentially impact many millions of consumers, we urge OMB to give the full and standard Federal Register notice period for any future comments in this area.

IX. Conclusion

Some portions of the Federal Register notice read part Pollyana, part commercial web site boilerplate privacy policy: "Technologies such as persistent cookies enable web sites to remember a visitor's preferences and settings, allowing for a more personalized, user-friendly experience." The government should not be conducting itself like a commercial venture, or even sounding like a commercial company.

The U.S. government needs to approach web development and consumer privacy with a different mind-set and different set of standards than a commercial company, understanding that consumer access to what is supposed to be publicly available government data or services should be unfettered by intrusive forms of web tracking, and especially tracking by third parties.

Ideally, the U.S. government will use its resources and influence to create better privacy online. We stand ready to assist with any questions you may have.

Respectfully submitted,

/s/

Pam Dixon
World Privacy Forum

Respectfully submitted,

Pam Dixon
Executive Director,
World Privacy Forum