

*Making the Rules, Breaking the Rules:*

**How the “White House for Kids”  
Web Site Violates  
Federal Privacy Policy**

A Special Report Issued by Privacilla.org

<http://www.privacilla.org>

©Privacilla.org. All content subject to the Privacilla Public License.

October, 2000

## Introduction

The Children's Online Privacy Protection Act was passed by Congress and signed by the President in October 1998. Its provisions took effect for all commercial Web sites directed at children earlier this year. In a June 2000 memorandum, Office of Management and Budget Director Jacob J. Lew set out Clinton Administration policy that all federal Web sites collecting information from children should comply with this privacy law.

Privacilla.org has found that the White House's own Web site does not follow Administration policy. Contrary to the Children's Online Privacy Protection Act, the "White House for Kids" site hosted at [www.whitehouse.gov](http://www.whitehouse.gov) collects personally identifiable information about children without getting verifiable parental consent. And it does not offer parents the opportunity to control their children's information.

The White House's own Web site does not follow Administration policy.

The "White House for Kids" Web site does not pose a serious danger to children. Nor did the commercial Web sites that stopped providing interaction and educational content to children when the Children's Online Privacy Protection Act took effect. The difficulty of applying the Children's Online Privacy Protection Act to just one leading federal Web site, however, shows how governments rob people of power over information about themselves and their children. It also suggests that future privacy laws and regulations should be studied much more carefully before being put into effect. On government or private-sector Web sites, they can be deeply burdensome and have dramatic unintended effects.

The White House should either stop collecting information from children on its Web site or rescind its privacy policy and admit that it cannot offer privacy protection to children. Regulators and political leaders everywhere should recognize with humility that their work often poses greater threats to privacy than private-sector businesses.

## The Children's Online Privacy Protection Act

Congress passed the Children's Online Privacy Protection Act (COPPA) as part of a giant omnibus spending bill in 1998. It was introduced and passed into law within the span of just a few months. COPPA received one hearing in the Senate and no separate consideration in the House of Representatives. The law took effect in April 2000.

COPPA requires "verifiable parental consent" before a commercial Web site operator may collect personally identifiable information from children. For the internal

use of the Web site, this means getting an e-mail from the parent. For other uses, this means talking to a parent, or getting postal mail, a fax, or a credit card number from a parent. COPPA also requires Web sites to allow parents to control their children's information in various ways. Violators of COPPA are subject to Federal Trade Commission enforcement action, including civil penalties of \$11,000 per violation.

The COPPA law singled out the Internet for special regulation and raised the cost of serving children online by \$50,000 to \$100,000 per Web site. On the Internet, which is driven by diversity and small business innovation, this is a lot. It means that new ways of teaching children will develop more slowly than they should, and competition for serving children will be thwarted. This month, for example, popular children's site Zeeks.com canceled its ZeekChat and ZeekMail services for kids. Popular television show *Thomas the Tank Engine* suspended its e-mail bulletins, to the disappointment of many children, in May.

More importantly, many children will lose access to valuable educational content and healthy online interaction. These will tend to be the children of poor, non-English-speaking, or absentee parents who can not or will not give consent. Other children will learn that lying about their ages gives them access to the worlds that other children enjoy.

## Questions About Government

While the federal government has been experimenting with children and Internet regulation, questions have been growing about the government itself. Because the U.S. government does not have its own house in order, it lacks authority to claim it can protect privacy. Indeed, it has a substantial role in undermining privacy and taking information-power away from people.

Recently, for example, a General Accounting Office report found that a staggering 97 percent of federal government Web sites do not adhere to the information practices that the Federal Trade Commission has recommended imposing on private-sector Web sites. As Office of Management and Budget Director Lew acknowledged by placing federal Web sites under COPPA, they should be at least as solicitous of privacy as private-sector Web sites. But "as good" is not good enough.

Federal Web sites should be at least as solicitous of privacy as private-sector Web sites. But "as good" is not good enough.

As Privacilla.org revealed in its September 2000 report, "*Assessing Threats to Privacy: The Government Sector — Greatest Menace to Privacy By Far*," governments

threaten privacy much more than the private sector does. Massive incentives push governments to collect, use, and store personal information about citizens. And they have few reasons to protect it. Example after example shows how governments threaten and invade privacy. The patchwork of laws that protect the public from government privacy invasions are insufficient.

Since at least 1996, the Office of Management and Budget has had a memorandum on “Management of Federal Information Resources” in place, intended to carry out the government’s responsibilities under the Privacy Act. In early June of this year, recognizing the growing concern with online privacy, the OMB issued a new memorandum dealing with “Privacy Policies on Federal Web Sites.”

Before the month was out, it came to light that the White House's Office of National Drug Control Policy was using cookies to track Web users who clicked on its anti-drug advertising. This prompted the OMB to issue another memorandum, this one entitled “Privacy Policies and Data Collection on Federal Web Sites.”

In addition to generally banning the use of cookies on federal Web sites, OMB Director Lew made it federal policy in this memorandum to apply the Children’s Online Privacy Protection Act to all federal Web sites. Specifically, OMB Memorandum M-00-13 (June 22, 2000)<sup>1</sup> said: “[I]t is federal policy that all Federal web sites and contractors when operating on behalf of agencies shall comply with the standards set forth in the Children's Online Privacy Protection Act of 1998 with respect to the collection of personal information online at web sites directed to children.”

### **How the “White House for Kids” Web Site Violates Federal Privacy Policy**

According to an analysis by Privacilla.org, the “White House for Kids” Web site hosted at [www.whitehouse.gov](http://www.whitehouse.gov) violates the Children’s Online Privacy Protection Act (COPPA) — and, therefore, Administration policy — in numerous ways. Foremost, it fails to get the required “verifiable parental consent” to collect children’s information online. The site does not even provide notice to parents that their children’s personal information is being collected and may be shared among government agencies.

“Verifiable parental consent” is the touchstone of the Children’s Online Privacy Protection Act. It is totally absent from the “White House for Kids” Web site. Though parents should have little to fear when their children send e-mail to the White House, the COPPA law was designed to empower parents, letting them alone decide with whom

---

<sup>1</sup> <http://www.whitehouse.gov/OMB/memoranda/m00-13.html>

their children may interact. In the absence of a “verifiable parental consent” procedure, there can be no honest claim that the COPPA law has been applied to the White House Web site.

Contrary to COPPA, parents of children who submit information to the White House Web site do not have any right to control that information. Correspondence may be archived under the Presidential Records Act (44 U.S.C. §2201 et seq.), and the White House privacy policy allows it to share information with other government agencies if the child’s inquiry relates to their work, or “as otherwise required by law.” All these provisions are inconsistent with COPPA, which requires Web sites to allow parents to refuse sharing of their children’s information with third parties. Moreover, parents may not review or delete their children’s information from White House records, which is required by COPPA. The White House’s privacy policy gives no information about who to contact with questions, another COPPA violation.

The “White House for Kids” Web site tips many hats to privacy, but in no way can it be said to comply with the Children’s Online Privacy Protection Act.

The “White House for Kids” Web site tips many hats to privacy, but in no way can it be said to comply with the Children’s Online Privacy Protection Act. The goal of that Act, parental empowerment, has no place when a child communicates with the White House via its World Wide Web site.

## Conclusion

It is easy to draw the wrong conclusions from privacy anecdotes. This example is no exception. However, a few tentative conclusions can be drawn.

First, the Children’s Online Privacy Protection Act appears overly prescriptive. By subjecting the White House Web site to the same privacy regulation that all private-sector businesses must follow, the Office of Management and Budget has illustrated for the world how difficult compliance with top-down regulatory schemes can be.

The White House Web site is one where most parents should probably feel comfortable allowing their children to visit and share information. It is probably unnecessary to apply the complicated COPPA law to the “White House for Kids” site, just as it was not needed on the majority of commercial Web sites. The operators of commercial Web sites directed to children know that their success relies on making parents and children comfortable and safe.

Second, government privacy regulations will carry substantial burdens and have unintended consequences. If put in place at all, they should not be rushed. The Children’s Online Privacy Protection Act was rushed through Congress, and the OMB’s decision to apply it to federal Web sites appears to have been rushed, too. If the law were actually implemented on the “White House for Kids” site, fewer children would interact with it and learn about our government. No one wants this, but it would be an inevitable result of political expedience on privacy. The politically expedient decision to impose COPPA on private-sector Web sites has already cut off healthy online interaction and learning for children.

Third, governments, as the biggest collectors and users of personal information, are not good stewards of privacy. Many, many government agencies collect personal information under the authority of law. To carry out their missions, they store it, share it, and use it in a variety of ways. Citizens have no choice as to whether they will share their personal information and no power over what is done with it. These are not the conditions that are likely to protect privacy.

The ability of the White House and OMB to manage the government is brought into question when the White House itself ignores a newly minted policy.

It is no surprise — and not necessarily a bad thing — that records from the White House Web site may be preserved for posterity or used in other ways. But every citizen should be aware that modern governments cannot carry out the many functions that inject them into the lives of citizens and, at the same time, protect privacy. Loss of privacy is one price of big government.

The final and surest conclusion is that the White House Web site should follow the Administration policy stated in Director Lew’s June 22 memorandum, or the policy should be changed and the Administration should admit that it will not protect children’s privacy by giving parents control. If the White House does not act, the federal agencies and the nation will get a clear signal that privacy protection is not an Administration priority and that OMB memoranda are not authoritative. The ability of the White House and OMB to manage the government is brought into question when the White House itself ignores a newly minted policy.

## Appendix

### Major COPPA Requirements Compared to “White House for Kids” Web Site<sup>2</sup>

| <i><b>Major COPPA Requirements<sup>3</sup></b></i>   | <i><b>“Write to the President”<sup>4</sup></b></i>  |
|--|---|
| <p><u>Who Must Comply</u><br/>If you operate a commercial Web site or an online service directed to children under 13 that collects personal information from children or if you operate a general audience Web site and have actual knowledge that you are collecting personal information from children, you must Comply with the Children's Online Privacy Protection Act.</p>  | <p>Though the site is non-commercial, OMB policy applies COPPA to all Federal Web sites. The site is directed to children.</p>                      |
| <p><u>Personal Information</u><br/>The Children's Online Privacy Protection Act and Rule apply to individually identifiable information about a child that is collected online, such as full name, home address, email address, telephone number or any other information that would allow someone to identify or contact the child. The Act and Rule also cover other types of information — for example, hobbies, interests and information collected through cookies or other types of tracking mechanisms — when they are tied to individually identifiable information.</p> | <p>Collects individually identifiable information: name, street address, city, state/province, zip or postal code, country, and e-mail address.</p> |
| <p><i><b>Privacy Notice</b></i></p>  |   |
| <p><u>Placement</u><br/>An operator must post a link to a notice of its information practices on the home page of its Web site or online service and at each area where it collects personal information from children. An operator of a general audience site with a separate children's area must post a link to its notice on the home page of the children's area.</p>   | <p>Privacy links appear on all relevant pages.</p>  |

<sup>2</sup> <http://www.whitehouse.gov/WH/kids/html/home.html>

<sup>3</sup> From “How to Comply With the Children’s Online Privacy Protection Rule”, <http://www.ftc.gov/bcp/conline/pubs/buspubs/coppa.htm>

<sup>4</sup> [http://www.whitehouse.gov/WH/kids/html/mail\\_pres.html](http://www.whitehouse.gov/WH/kids/html/mail_pres.html)

|  |  |
|--|--|
| <p>The link to the privacy notice must be clear and prominent. Operators may want to use a larger font size or a different color type on a contrasting background to make it stand out. A link in small print at the bottom of the page — or a link that is indistinguishable from other links on your site — is not considered clear and prominent.</p>   | <p>Though privacy link on “White House for Kids” home page is at bottom of page, it is slightly larger than other type. At “Write to the President” page, link is prominent.</p> |
| <p><u>Content</u><br/>The notice must be clearly written and understandable; it should not include any unrelated or confusing materials. It must state the following information:</p>  | <p>Satisfactory.</p>   |
| <ul style="list-style-type: none"> <li>• The name and contact information (address, telephone number and email address) of all operators collecting or maintaining children's personal information through the Web site or online service. If more than one operator is collecting information at the site, the site may select and provide contact information for only one operator who will respond to all inquiries from parents about the site's privacy policies. Still, the names of all the operators must be listed in the notice.</li> </ul> | <p>No information given.</p>   |
| <ul style="list-style-type: none"> <li>• The kinds of personal information collected from children (for example, name, address, email address, hobbies, etc.) and how the information is collected — directly from the child or passively, say, through cookies.</li> </ul>  | <p>Yes.</p>  |
| <ul style="list-style-type: none"> <li>• How the operator uses the personal information. For example, is it for marketing back to the child? Notifying contest winners? Allowing the child to make the information publicly available through a chat room?</li> </ul>  | <p>Yes.</p>  |
| <ul style="list-style-type: none"> <li>• Whether the operator discloses information collected from children to third parties. If so, the operator also must disclose the kinds of businesses in which the third parties are engaged; the general purposes for which the information is used; and whether the third parties have agreed to maintain the confidentiality and security of the information.</li> </ul>   | <p>A link to the text of the Presidential Records Act does not inform parents. Sharing with other agencies or “as . . . required by law” is noted, but not described.</p>        |
| <ul style="list-style-type: none"> <li>• That the parent has the option to agree to the collection and use of the child's information without consenting to the disclosure of the information to third parties.</li> </ul>   | <p>No. The parent may not control use of the child's information once it is submitted.</p>   |



|  |  |
|--|--|
| <ul style="list-style-type: none"> <li>• That the operator may not require a child to disclose more information than is reasonably necessary to participate in an activity as a condition of participation.</li> </ul>   | No information given.  |
| <ul style="list-style-type: none"> <li>• That the parent can review the child's personal information, ask to have it deleted and refuse to allow any further collection or use of the child's information. The notice also must state the procedures for the parent to follow.</li> </ul>  | The parent has neither the right to review or delete information, nor refuse further collection or use.  |
| <b><i>Direct Notice to Parents</i></b>   |  |
| <p><u>Content</u><br/>The notice to parents must contain the same information included on the notice on the Web site. In addition, an operator must notify a parent that it wishes to collect personal information from the child; that the parent's consent is required for the collection, use and disclosure of the information; and how the parent can provide consent. The notice to parents must be written clearly and understandably, and must not contain any unrelated or confusing information. An operator may use any one of a number of methods to notify a parent, including sending an email message to the parent or a notice by postal mail.</p> | Information is collected without assurance of notice to parents. Children are encouraged to ask parents. |
| <p><u>Verifiable Parental Consent</u><br/>Before collecting, using or disclosing personal information from a child, an operator must obtain verifiable parental consent from the child's parent. This means an operator must make reasonable efforts (taking into consideration available technology) to ensure that before personal information is collected from a child, a parent of the child receives notice of the operator's information practices and consents to those practices.</p>   | Verifiable parental consent is not obtained before information is collected.                             |
| <p><u>Internal Uses</u><br/>Operators may use email to get parental consent for all internal uses of personal information, such as marketing back to a child based on his or her preferences or communicating promotional updates about site content, as long as they take additional steps to increase the likelihood that the parent has, in fact, provided the consent. For example, operators might seek confirmation from a parent in a delayed confirmatory email, or confirm the parent's consent by letter or phone call.</p>  | No consent is obtained.  |

|  |  |
|--|--|
| <p><u>Public Disclosures</u></p> <p>When operators want to disclose a child’s personal information to third parties or make it publicly available (for example, through a chat room or message board), the sliding scale requires them to use a more reliable method of consent, including: getting a signed form from the parent via postal mail or facsimile; accepting and verifying a credit card number in connection with a transaction; taking calls from parents, through a toll-free telephone number staffed by trained personnel; email accompanied by digital signature.</p> | <p>No consent is obtained.</p>   |
| <p><u>Disclosures to Third Parties</u></p> <p>An operator must give a parent the option to agree to the collection and use of the child's personal information without agreeing to the disclosure of the information to third parties. However, when a parent agrees to the collection and use of their child's personal information, the operator may release that information to others who uses it solely to provide support for the internal operations of the website or service, including technical support and order fulfillment.</p>  | <p>No consent is obtained.</p>   |
| <p><u>Exceptions</u></p> <p>The regulations include several exceptions that allow operators to collect a child's email address without getting the parent's consent in advance. These exceptions cover many popular online activities for kids, including contests, online newsletters, homework help and electronic postcards. Prior parental consent is not required when:</p>   | <p>No exceptions apply. Site collects information beyond e-mail addresses.</p> |
| <ul style="list-style-type: none"> <li>• an operator collects a child's or parent's email address to provide notice and seek consent;</li> </ul>   | <p>N/A</p>   |
| <ul style="list-style-type: none"> <li>• an operator collects an email address to respond to a one-time request from a child and then deletes it;</li> </ul>   | <p>N/A</p>   |
| <ul style="list-style-type: none"> <li>• an operator collects an email address to respond more than once to a specific request — say, for a subscription to a newsletter. In this case, the operator must notify the parent that it is communicating regularly with the child and give the parent the opportunity to stop the communication before sending or delivering a second communication to a child;</li> </ul>   | <p>N/A</p>   |

|   |  |
|---|--|
| <ul style="list-style-type: none"> <li>• an operator collects a child's name or online contact information to protect the safety of a child who is participating on the site. In this case, the operator must notify the parent and give him or her the opportunity to prevent further use of the information;</li> </ul>   | N/A  |
| <ul style="list-style-type: none"> <li>• an operator collects a child's name or online contact information to protect the security or liability of the site or to respond to law enforcement, if necessary, and does not use it for any other purpose.</li> </ul>   | N/A  |
| <p><u>New Notice for Consent</u><br/> An operator is required to send a new notice and request for consent to parents if there are material changes in the collection, use or disclosure practices to which the parent had previously agreed. Take the case of the operator who got parental consent for a child to participate in contests that require the child to submit limited personal information, but who now wants to offer the child chat rooms. Or, consider the case of the operator who wants to disclose the child's information to third parties who are in materially different lines of business from those covered by the original consent — for example, marketers of diet pills rather than marketers of stuffed animals. In these cases, the Rule requires new notice and consent.</p>  | No consent is obtained.  |
| <p><u>Access Verification</u><br/> At a parent's request, operators must disclose the general kinds of personal information they collect online from children (for example, name, address, telephone number, email address, hobbies), as well as the specific information collected from children who visit their sites. Operators must use reasonable procedures to ensure they are dealing with the child's parent before they provide access to the child's specific information. They can use a variety of methods to verify the parent's identity, including: obtaining a signed form from the parent via postal mail or facsimile; accepting and verifying a credit card number; taking calls from parents on a toll-free telephone number staffed by trained personnel; email accompanied by digital signature; email accompanied by a PIN or password obtained through one of the verification methods above.</p> | Parents may learn for themselves what information is collected. No mechanism appears to provide child-specific information to parents. |

|   |   |
|---|---|
| <p><u>Revoking &amp; Deleting</u></p> <p>At any time, a parent may revoke his/her consent, refuse to allow an operator to further use or collect their child's personal information, and direct the operator to delete the information. In turn, the operator may terminate any service provided to the child, but only if the information at issue is reasonably necessary for the child's participation in that activity. For example, an operator may require children to provide their email addresses to participate in a chat room so the operator can contact a youngster if he is misbehaving in the chat room. If, after giving consent, a parent asks the operator to delete the child's information, the operator may refuse to allow the child to participate in the chat room in the future. If other activities on the Web site do not require the child's email address, the operator must allow the child access to those activities.</p> | <p>Parent has no right to revoke consent, refuse further collection, or require the operator to delete information.</p> |
|---|---|