California Requires Online Privacy Policies, Prompting Changes to Websites

2004-08-09

California has enacted the first state law requiring website operators to post privacy policies on their websites, and the law is not limited to California-based companies. California's Online Privacy Protection Act of 2003 (OPPA)became effective on July 1, 2004, and applies to all businesses that have a commercial website or online service reaching consumers in California. Although many companies already maintain privacy policies on their websites in order to comply with generally accepted Fair Information Practices (see our previous Email Alert of May 2, 2000, FTC Raises Its Profile on E-Privacy Issues), the new California law imposes specific requirements concerning both the form and the content of a website privacy policy. Even with possible constitutional challenges looming, OPPA is already prompting website operators to reassess their online privacy practices.

OPPA requires each business that collects personally identifiable information from California consumers through its commercial website or online service to "conspicuously post" a privacy policy on its website. This means that the actual text of the privacy policy must appear on the homepage or the first significant page after entering the site, or must be accessible through a hyperlink, text link or other functional link, as follows:

- If a company uses an icon as a hyperlink, it must be included on the homepage or first significant page of the website, must include the word "privacy," and must also use a color that contrasts with the background color of the page.
- If a company uses a text link, it must either include the word "privacy;" be written in capital letters equal to or greater in size than the surrounding text; or be "written in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the language."
- If a company uses some other functional link, it must be displayed so that a "reasonable person" would notice it. In the case of an online service, the privacy policy must be "reasonably accessible."

The privacy policy must include the following information:

- The categories of personal information that will be collected through the site or service--

personal information includes first and last name, street address, email address, telephone number, social security number, any other identifier by which a person can be contacted physically or online, and any other information that is collected from the user and maintained in an identifiable form

- The categories of third parties with whom this personal information may be shared
- A description of the process by which consumers can review or request changes to the personal information, if any such process exists
- A description of the process by which consumers will be notified of any material changes to the privacy policy
- The effective date of the policy

A company that fails to provide the appropriate information in its privacy policy may be liable for violations of the law if its failure to comply is either "knowing and willful" or "negligent and material." Companies that are notified of noncompliance will have 30 days to comply. A failure to comply with these requirements could lead to civil fines or injunctions.

While the new law is a California statute, it may affect any website that can be viewed by California consumers, which is, effectively, every company with a commercial website or online service. Companies that already have privacy policies posted on their websites may need to evaluate whether these policies are sufficiently accessible and contain the required information.

Changing a privacy policy to conform to the California law might raise additional legal risks. The Federal Trade Commission (FTC) recently announced a proposed settlement with Gateway Learning Corporation, the company that markets "Hooked on Phonics." Gateway's privacy policy indicated that the company would not "sell, rent or loan any personally identifiable information . . . with any third party...,"but explicitly reserved the right to change its policy with notice "on this Site or by e-mail." Gateway later changed its policy to permit the sale of personal information, but did not send email notifications or indicate on its website that its policy had changed. When the company applied the *new* policy to previously gathered personal information, the FTC charged that the retroactive application of a materially changed policy was an unfair practice and that the failure to notify consumers of the change was a deceptive practice.

Thus, at a minimum, any material changes to a privacy policy must be announced in accordance with the policy-change process specified in the original policy. Even then, consumers may be entitled to notice and a choice before such changes may be applied to previously collected data. As part of the Gateway settlement, the FTC required "explicit, opt-in" consent, consistent with Gateway's original policy. In other situations, adequate notice and an opportunity to "opt out" may be sufficient. This determination requires a careful, case-by-case review of the policy being changed.

Contributors

Barry J. Hurewitz

PARTNER