

AVOIDING PRIVACY LITIGATION

Practical Checklist to Help Prevent Litigation

THE BACKGROUND BASICS: SOLID PRIVACY PRACTICES START WITH A GOOD PRIVACY POLICY

- ✍ Develop and maintain a privacy policy. If you have any doubts about whether developing a policy is worth the investment, consider the following issues:
 - ✍ the FTC wants you to have one,
 - ✍ it will almost certainly be required by law soon,
 - ✍ the policy may protect you in litigation,
 - ✍ consumer backlash on privacy issues is an increasing issue and is not likely to go away.

- ✍ You cannot be too scrupulous. Follow your privacy policy with utmost care. Most of the lawsuits in the on-line arena arise based on allegations the company is not complying with its own stated policy.

WHAT SHOULD BE INCLUDED IN YOUR PRIVACY POLICY?

- ✍ At a minimum, your policy should include the following elements:
 - ✍ whether your site collects personal information,
 - ✍ what information is collected,
 - ✍ how information is collected,
 - ✍ how the information may be used,
 - ✍ whether the information is shared with third parties,
 - ✍ a method by which users can opt-out if information is shared with third parties,
 - ✍ a provision allowing consumers to review collected information upon request,
 - ✍ a provision allowing consumers to request removal or changes to the information, and
 - ✍ information on how your site protects private customer information.

- ✍ Reserve the right to disclose personal information under the following circumstances: to comply with applicable laws and lawful government requests, to ensure proper operation of your systems, and to protect yourself and/or your users.

- ✍ Be aware of the activities of third-party content providers on your site. In particular, disclose if third-party content providers are using cookies.

- ✍ If you enter into co-branding relationships in which both partners have access to consumer information, disclose that other companies have access to the consumer's information and disclaim liability on your site for any and all of your co-branded partner's information gathering practices.

- ✍ Include language in the privacy policy to make it clear that the policy applies to any acquiring third party. Consider defining “the company” to include “any successors and assignees.”
- ✍ Include a statement in the privacy policy that the policy may be amended at any time without notice.
- ✍ Nevertheless, if you do significantly amend your privacy policy, consider sending out a notice to your consumers.
- ✍ If your site includes links to other sites, include a disclaimer regarding all material on sites outside of your control.
- ✍ Make sure you update your privacy policy to reflect new technology and practices.
- ✍ If you have partnership agreements which allow you to frame other sites (or vice versa), consider whether there is a conflict between your privacy policy and that of your partners. Likewise, consider the privacy policies of your third-party content providers and think about whose policy applies on your site.
- ✍ Be sure the link to your privacy policy is “clear and conspicuous.” Make sure it appears on your home page and is not hidden.
- ✍ If you accept banner ads, include a disclaimer of their activities.

AUGMENT AND SUPPORT YOUR PRIVACY POLICY WITH GOOD BUSINESS PRACTICES

- ✍ Limit the number of company spokespersons and instruct everyone to refer all outside inquiries to an official spokesperson.
- ✍ Be aware of what consumers are saying about your privacy practices. Some companies employ an outside PR firm to monitor online forums with respect to consumer backlash.
- ✍ Consider emphasizing your commitment to good privacy practices by creating room for “privacy” personnel in your corporate structure. Some companies, such as DoubleClick, have created privacy boards and others, such as [Excite@home](#), have established chief privacy officers.
- ✍ Educate everyone in your company about your privacy policies and the laws governing consumer data. This can be effectively combined with antitrust and securities compliance training.
- ✍ Develop a written insider privacy policy. Distribute the policy to every employee and have them sign it.

- ✍ Create a corporate e-mail policy delineating protocols for communicating with users. The policy should address the various types of communication the company may send, such as informational newsletters, service e-mails, corporate e-mails and third-party newsletters. Consider addressing the appropriate frequency of such e-mails.
- ✍ Send out periodic reminders to employees about the privacy policy.
- ✍ Be wary of the problem of leaked internal e-mail. Strictly and explicitly prohibit forwarding of consumer or other e-mail outside the company.
- ✍ Develop and maintain a written e-mail retention policy.
- ✍ Institute a web-review policy requiring periodic review of the site for outdated or inaccurate information.
- ✍ Consider the advantages (and disadvantages) of membership in one of the self-enforcement programs such as TRUSTe or BBBOnline. These programs will help you create and maintain privacy policies. They will also help you comply with COPPA (discussed below). If a company participates and complies with a commission-approved self-enforcement program, COPPA provides a safe harbor in the event of an enforcement action.

KEEP UPDATED ON THE STATE OF THE LAW

- ✍ Make sure that you are actively monitoring the privacy laws; this is one area where the law will almost certainly change in the near future.
- ✍ Be aware of the Children’s Online Privacy Protection Act of 1998 (COPPA), which sets forth rules and procedures about how web sites can collect, use and disclose personal information about children under the age of 13. COPPA applies to two kinds of web sites: commercial sites directed or targeted towards children and “general audience” sites whose operators have actual knowledge that they are collecting personal information from children.
 - ✍ Notice: COPPA sites must disclose their information gathering practices with respect to children in a “clear and prominent” page on the site’s home page. The site must repeat this disclosure at every additional area where personal information is requested. The notice must include the following:
 - ✍ contact information for operators collecting personal information;
 - ✍ a description of the personal information collected;
 - ✍ a description of the way the personal information may be used;
 - ✍ a statement that a child’s participation in a contest, promotion or sweepstakes will not be conditioned on the disclosure of more personal information than is necessary to participate in the activity; and

- ✍ a statement informing parents of their right to review and/or delete their child's information as well as revoke any prior consent at any time.
- ✍ **VERIFIABLE PARENTAL CONSENT:** A COPPA site must obtain verifiable parental consent before it collects, uses or discloses personal information from children under the age of 13.
- ✍ Consider whether you fall into the broad definition of "financial institution" under the new Gramm-Leach-Bliley Act, Pub. L. 106-102. This Act limits the instances in which a financial institution may disclose nonpublic personal information to nonaffiliated third parties, and requires financial institutions to disclose the institution's privacy policies and practices with respect to information sharing with both affiliates and non-affiliated third parties. The FTC's final privacy rule, 16 CFR 313, was effective November 13, 2000. Full compliance is required by July 1, 2001. The Act and the FTC rule are complex and detailed and if you are a financial institution, you should now undertake a comprehensive compliance review with respect to this legislation.
- ✍ Consider whether the December 28, 2000 Final Regulations on Standards for Privacy of Individually Identifiable Health Information (HIPPA privacy rules) apply to your company. This rule establishes standards to protect the privacy of individually identifiable health information maintained or transmitted in connection with certain administrative and financial transactions. The rule applies to health plans, health care clearinghouses, and certain health care providers. It sets privacy standards to protect individuals, as well as procedures for the exercise of those rights and disclosures of information. The rule becomes effective on February 26, 2001 and compliance is required two years thereafter for covered entities. Like the Gramm-Leach-Bliley Act, the HIPPA requirements are complex and detailed. If you are a covered entity, you should now undertake a comprehensive compliance review.
- ✍ If applicable, create a procedure for responding to subpoenas for user identification. Section 7 of the Electronic Communications Privacy Act of 1986 requires a court order to be issued in order for a provider of electronic communication service or remote computing service to disclose the contents of an electronic communication or records or other information pertaining to a subscriber or customer. Although the Act only applies to governmental entities, many internet companies adhere to similar rules when responding to requests for user information from private third parties. Make a clear policy whether you provide notice to users when you receive a subpoena requesting their information in order to allow the user to quash the subpoena.