

LOS ANGELES

# Daily Journal

WEDNESDAY,  
DECEMBER 13, 2006

— SINCE 1888 —

OFFICIAL NEWSPAPER OF THE LOS ANGELES SUPERIOR COURT AND UNITED STATES SOUTHERN DISTRICT COURT

## Focus

# Privacy Policies

By Alan L. Friel

Not so many years ago, companies needed only to follow their own privacy policies to avoid running afoul of the law. But those days are long gone. Online and off-line privacy issues are some of the hottest political and consumer issues of late, leading to broad state and federal regulation of how companies collect and use consumer information. The lawyer has the responsibility of helping clients deal with consumers' personal information and implement appropriate policies and procedures to protect that data.

Congress has passed consumer privacy laws concerning financial institutions and credit data, medical data, and personal information regarding young children. Although specific federal legislation governing more general types of information has not been passed, privacy policies are considered advertising claims regulated by the Federal Trade Commission. To avoid FTC enforcement, they must not be inaccurate, deceptive or unfair. Further, the FTC has found that the failure to have a privacy policy and to maintain industry standard data security measures is itself an unfair or misleading advertising practice.

California has enacted legislation more far-reaching than federal law. Commercial Web sites and online services that collect personally identifiable information from California consumers must have a privacy policy that complies with Business and Professions Code Section 22575, the Online Privacy Protection Act.

In addition, if personal information is collected online or off-line, and disclosed to direct marketers, Civil Code Section 1798.83, the Shine the Light law, requires businesses to give notice and explanation of consumers' rights. Unless the business has a policy and procedures compliant with the act, and a cost-free method to prevent sharing, it must keep disclosure data and give it to consumers on request.

In addition, California law requires that companies maintain reasonable security measures and practices to protect and destroy personal information. If certain personal information of California residents is kept, Section 1798.82

requires that businesses must follow certain notice requirements in the event of a security breach.

California law also has special requirements and prohibited actions with respect to Social Security numbers, information encoded on driver's licenses, medical, insurance and utility information, income tax returns, video sales or rental information and information regarding collection actions against identity-theft victims.

### Information About Kids

If a Web site is directed to, or attractive to, children younger than 13, or if a Web site operator has actual knowledge that it is collecting or publishing (for example, through user-generated content or chat rooms) personal information of children younger than 13, the federal Child Online Privacy Protection Act has special requirements that must be followed. If the site is clearly for users older than 13, a privacy policy should explain that there is no intention to collect personal information from young children, provide parents with a method to remove inadvertently obtained information and the site should also take measures to prevent knowing collection of personal information of children younger than 13.

### Policy Contents

Like any consumer contract, a privacy policy should use plain language and avoid technical jargon. Use short sentences and active-voice verbs. Select a readable font in a legible size. Format the policy to let a user print it from the Web site.

The privacy policy should have a descriptive title containing the word "privacy" in legible type designed to highlight its significance. If relating to a Web site, the policy must be posted conspicuously on the site, with a "privacy" link on the home page and every Web page where personal information is collected.

Corporate Web sites should make privacy policies available covering both off-line and online practices for managing personal information or be specific that only online practices are addressed by the posted policy. The policy should indicate which entities it covers, such

as subsidiaries or affiliates. It also should state that the site is directed only to users in the United States and that only this country's laws govern.

If personal information is shared with third-party direct marketers, the Web site's home page must have a link titled "Your Privacy Rights," in a prominent font that links to a summary of consumers' legal rights and provides the company's contact information. This link may be to the company's privacy policy so long as the first page of the policy gives consumers the required notices in a manner no less prominent than the rest of the policy. If the link uses the words "Your California Privacy Rights" and links to a compliant privacy policy, the company need only respond to consumer requests that are to the contact listed for such in the policy.

In addition, if either form of the link is to a policy that explains the right to prevent sharing of information for direct marketing and allows a free method to prevent such sharing, the company need not respond to consumer inquiries about with which all their information has been shared. If the company does not offer such an "opt-out" or "opt-in" method, it must make disclosure information available at every place of business in California where the business or its agents regularly have contact with California consumers.

The privacy policy should be specific in describing all of the kinds of personal information collected. At the least, it must list the categories of information that are collected from Web site visitors. For example, "We collect contact information, such as your name, IP address and e-mail address, as well as billing information, such as credit card number and billing address."

The privacy policy should explain all sources for the collection of personal information, including from sources other than customers themselves. It also should explain what types of Web technologies, such as log files, cookies or Web beacons (called clear GIFs), collect information. Consider explaining the use of cookies by ad networks that serve ads on the site and linking to the opt-out program of those networks participating in the Network Advertising Initia-

tive ([www.networkadvertising.org](http://www.networkadvertising.org)).

The privacy policy should explain all uses of personal information beyond what is necessary for fulfilling a customer transaction. It should explain practices regarding information sharing with others. At the very least, the privacy policy must list the types of parties with which the company shares customers' personal information. If any other parties have a direct link or live feed of consumer information through a Web site, the policy should say so.

Many companies assume that they will never share collected information, and they make an categorical statement to this effect. This can cause serious problems when circumstances change. The policy should provide for the right to transfer in event of change of control, sale or merger.

The privacy policy should give at least a title and e-mail or postal address of a company official who will respond to privacy questions and requests. Best practices and FTC guidelines recommend offering a process for consumers to review and change their personal information. Business and Professions Code Section 22575(b)(2) requires operators of commercial Web sites and online services to describe the process for reviewing and correcting personal information, where such a process is offered.

The privacy policy should give a general description of the security measures used to safeguard the personal information, but not in such detail as to compromise security. The company's security measures should meet state and federal standards. Companies should consider following the FTC and Better Business Bureau security guidelines and those of the various pri-

ivate secure-site rating services. In addition, the company should require third parties with which data is shared to use it only as permitted and to maintain best practices to protect the data and to comply with all laws and to inform the company promptly of any suspected or actual misuse or security breach.

The privacy policy should explain what will happen in the case of a security breach. A company can, in its policy, create an ability to give notice by cost-efficient methods such as e-mail or posting a notice on the home page rather than the more-burdensome methods otherwise required by California law.

The Business and Professions Code requires operators of commercial Web sites and online services to provide a policy effective date and requires operators of commercial Web sites and online services to explain how they notify consumers of material changes to the policy. A company must obtain consumer consent before it can start using the previously collected information in a materially different manner. If consumers are not opting in to a new policy, the company should continue to treat information collected under the old policy under that policy.

#### **Opting Out**

Compliance with California law will be easier with a simple, effective way for consumers to consent to, or to opt out of, sharing their personal information with other parties. When a consumer opts out, the company should implement the consumer's preferences within a reasonable time, such as within five to ten business days.

The explanation of the opt-out procedure

should explain clearly the extent of a consumer's option to limit sharing of personal information. It is a good idea to provide an acknowledgment or confirmation of a consumer's request not to have personal information shared. The policy also should explain that, despite an opt-out, there may remain nonmarketing reasons for sharing information or contacting customers, such as product safety, customer service, completing a requested transaction and compliance with law and law enforcement compliance.

Finally, the policy should not confuse the opt-out of information sharing with the consumer's federal statutory right under the CAN SPAM Act to opt out of receiving commercial e-mails. A privacy policy also may include information on CAN SPAM opt-outs, but the types of consumer action should be explained and segregated.

For further information on industry best practices regarding consumer privacy and privacy policies, see Direct Marketing Association Guidelines ([www.the-dma.org/privacy](http://www.the-dma.org/privacy)), American Institute of CPAs/CICA Privacy Framework ([infotech.aicpa.org/resources/privacy](http://infotech.aicpa.org/resources/privacy)), Better Business Bureau Privacy Seal guidelines ([www.bbbonline.org/privacy](http://www.bbbonline.org/privacy)) and Article 19 of the Consolidated Code of Advertising and Marketing Communications Practice of The International Chamber of Commerce ([www.iccwbo.org/display/doctype6/index.html](http://www.iccwbo.org/display/doctype6/index.html)).

---

**Alan L. Friel** is counsel at Kaye Scholer in Los Angeles, where he advises companies in the entertainment, technology, advertising and new media industries. Mr. Friel can be reached at 310.788.1052 or [afriel@kayescholer.com](mailto:afriel@kayescholer.com).